PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-274791
(43)Date of publication of application : 05.10.2001

(51)Int.Cl. H04L 9/32
G06F 12/14
G09C 1/00
H04L 9/08

(21)Application number : 2000-087445
(22)Date of filing : 27.03.2000

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : KAWADA KOJI
KATSUTA NOBORU

(54) DEVICE AUTHENTICATION METHOD, DEVICE AUTHENTICATION SYSTEM, RECEIVER AND TRANSMITTER

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a device authentication system that can exclude an illicit receiver.
SOLUTION: In a player 100, selection section 102 selects any of sets each consisting of address data, extended address data and key data stored in a storage section 101, transmission section 103 transmits the address data, conversion section 105 converts the extended address data into 1st data, and transmission section 106 transmits the 1st data. In a key media 150, reception sections 152, 157 receive them, an extraction section 153 extracts the extended address data, from the extended address data including addresses stored in a storage section 151, a conversion section 156 converts the extended address data into 2nd data, a verification section 158 verifies whether the 1st data are identical to the 2nd data, an extraction section 160 extracts encrypted data from a plurality of encrypted data with the extended addresses stored in a storage section 159, when they are the same, and a transmission section 161 transmits the extracted data. In the player 100, a reception section 908 receives the

encrypted data, and a decoding section 108 decodes the data by using the key data.

LEGAL STATUS

[Date of request for examination] 21.12.2006

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] By transmitting the data for an encryption communication link with which the data for a communication link were enciphered to a receiving set from a sending set, and decrypting before cryptocommunication, the data for an encryption communication link which the receiving set received using the key data for double signs which self holds A receiving set shares the data for a communication link which a sending set memorizes beforehand, and this actuation is followed. It is the device authentication approach in the cryptocommunication system which performs cryptocommunication using the shared data for a communication link. Said receiving set One sets or more of data sets which consist of the 1st address data, the 2nd address data, and key data for decode are memorized beforehand. Said sending set The 2nd address data with the 1st address which can specify the 2nd address data from the 1st address data, The data for the encryption communication link with the 2nd address which can specify the data for an encryption communication link from the 2nd address data The 1st address-data transmission step which transmits the 1st address data belonging to the data set of one of the data sets which have memorized beforehand, respectively and said receiving set memorizes from said receiving set

beforehand to said sending set, [two or more] In said sending set, from two or more 2nd address data with the 1st address memorized beforehand The 2nd address-data extract step which extracts the 2nd address data specified with the 1st address data transmitted by said 1st address-data transmission step from said receiving set, The 2nd address data belonging to said data set of 1 in said receiving set, The verification step to which the 2nd address data extracted by said 2nd address-data extract step in said sending set verify whether it is the same value, When it is verified by said verification step that it is the same value, it sets to said sending set. From two or more data for the encryption communication link with the 2nd address memorized beforehand The data extraction step for an encryption communication link which extracts the data for an encryption communication link specified with the 2nd address data extracted by said 2nd address-data extract step, In the data transmission step for an encryption communication link which transmits the data for an encryption communication link extracted by said data extraction step for an encryption communication link to said receiving set from said sending set, and said receiving set The device authentication approach characterized by having the decryption step which decrypts the data for an encryption communication link transmitted by said data transmission step for an encryption communication link using the key data for decode belonging to said data set of 1, and generates the data for a communication link.

[Claim 2] Said verification step The inside of said receiving set, Or by transmitting the random-number data which were made to generate random-number data and were generated within said sending set to another side In the random-number data sharing substep which shares the same random-number data, and said receiving set Predetermined data conversion is performed to the 2nd address data belonging to said data set of 1, and said shared random-number data. In the 1st data-conversion substep which generates the data for the 1st verification, the data transmission substep for the 1st verification which transmits said data for the 1st verification to said sending set from said receiving set, and said sending set The 2nd address data extracted by said 2nd address-data extract step, In the 2nd data-conversion substep which performs the same data conversion as said 1st data-conversion substep to said shared random-number data, and generates the data for the 2nd verification to them, and said sending set The device authentication approach according to claim 1 that said data for the 1st verification and said data for the 2nd verification are characterized by having the verification substep which verifies whether it is the same value.

[Claim 3] By transmitting the data for an encryption communication link with which the data for a communication link were enciphered to a receiving set from a sending set, and decrypting before cryptocommunication, the data for an encryption communication link which the receiving set received using the key data for decode which self holds A receiving set shares the data for a communication link which a

sending set memorizes beforehand, and this actuation is followed. It is the device authentication system which performs cryptocommunication using the shared data for a communication link and which consists of a sending set and a receiving set. Said receiving set A data set storage means to memorize beforehand one sets or more of data sets which consist of the 1st address data, the 2nd address data, and key data for decode, A 1st address-data transmitting means to transmit the 1st address data belonging to the data set of one of the data sets memorized by said data set storage means to said sending set, Carry out based on the 2nd address data belonging to said data set of 1, and predetermined data conversion is performed. A 1st data-conversion means to generate the data for the 1st verification, and a data transmitting means for the 1st verification to transmit said data for the 1st verification to said sending set, A data receiving means for an encryption communication link to receive the data for an encryption communication link from said sending set, The data for an encryption communication link received by said data receiving means for an encryption communication link It has a decryption means to decrypt using the key data for decode belonging to said data set of 1, and to generate the data for a communication link. Said sending set The 2nd address data with the 1st address which can specify the 2nd address data from the 1st address data, A set storage means to memorize beforehand two or more data for the encryption communication link with the 2nd address which can specify the data for an encryption communication link from the 2nd address data, respectively, A 1st address-data receiving means to receive the 1st address data from said receiving set, From two or more 2nd address data with the 1st address memorized by said set storage means A 2nd address-data extract means to extract the 2nd address data specified with the 1st address data received by said 1st address-data receiving means from said receiving set, A data receiving means for the 1st verification to receive said data for the 1st verification from said receiving set, It carries out based on the 2nd address data extracted by said 2nd address-data extract means. A 2nd data-conversion means to perform the same data conversion as said 1st data-conversion means, and to generate the data for the 2nd verification, A verification means by which the data for the 1st verification received by said data receiving means for the 1st verification and the data for the 2nd verification generated by said 2nd data-conversion means verify whether it is the same value, When it is verified by said verification means that it is the same value, from two or more data for the encryption communication link with the 2nd address memorized beforehand A data extraction means for an encryption communication link to extract the data for an encryption communication link specified with the 2nd address data extracted by said 2nd address-data extract means, The device authentication system characterized by having a data transmitting means for an encryption communication link to transmit the data for an encryption communication link extracted by said data extraction means for an encryption communication link to said receiving set.

[Claim 4] Said 1st data-conversion means with which said receiving set is equipped

From said sending set, a random-number data receiving means to receive random-number data is included. Said 1st data-conversion means It carries out based on the 2nd address data belonging to said data set of 1, and the random-number data received by said random-number data receiving means. Said 2nd data-conversion means with which performs predetermined data conversion, and generates the data for the 1st verification, and said sending set is equipped A random-number data generating transmitting means to transmit the random-number data which were made to generate random-number data and were generated to said receiving set is included. Said 2nd data-conversion means The device authentication system according to claim 3 which carries out based on the 2nd address data extracted by said 2nd address-data extract means, and the random-number data generated with said random-number data generating transmitting means, and is characterized by performing predetermined data conversion and generating the data for the 2nd verification.
[Claim 5] Said 1st data-conversion means with which said receiving set is equipped Said random-number data generating transmitting means to transmit the random-number data which were made to generate random-number data and were generated to said sending set is included. Said 1st data-conversion means It carries out based on the 2nd address data belonging to said data set of 1, and the random-number data generated with said random-number data generating transmitting means. Said 2nd data-conversion means with which performs predetermined data conversion, and generates the data for the 1st verification, and said sending set is equipped From said receiving set, a random-number data receiving means to receive random-number data is included. Said 2nd data-conversion means The device authentication system according to claim 3 which carries out based on the 2nd address data extracted by said 2nd address-data extract means, and the random-number data received by said random-number data receiving means, and is characterized by performing predetermined data conversion and generating the data for the 2nd verification.
[Claim 6] By transmitting the data for an encryption communication link with which the data for a communication link were enciphered to a receiving set from a sending set, and decrypting before cryptocommunication, the data for an encryption communication link which the receiving set received using the key data for decode which self holds A receiving set shares the data for a communication link which a sending set memorizes beforehand, and this actuation is followed. It is a receiving set in the device authentication system which performs cryptocommunication using the shared data for a communication link. A data set storage means to memorize beforehand one sets or more of data sets which consist of the 1st address data, the 2nd address data, and key data for decode, A 1st address-data transmitting means to transmit the 1st address data belonging to the data set of one of the data sets memorized by said data set storage means to said sending set, Carry out based on the 2nd address data belonging to said data set of 1, and predetermined data conversion is performed. A data-conversion means to generate the data for

verification, and a data transmitting means for verification to transmit said data for verification to said sending set, A data receiving means for an encryption communication link to receive the data for an encryption communication link from said sending set, The receiving set characterized by having a decryption means to decrypt the data for an encryption communication link received by said data receiving means for an encryption communication link using the key data for decode belonging to said data set of 1, and to generate the data for a communication link.
[Claim 7] Said data-conversion means is a receiving set according to claim 6 characterized by carrying out based on the 2nd address data belonging to said data set of 1, and the random-number data received by said random-number data receiving means, performing predetermined data conversion, and generating the data for verification including a random-number data receiving means by which said data-conversion means receives random-number data from said sending set.
[Claim 8] Said data-conversion means is the receiving set according to claim 6 characterized by to carry out based on the 2nd address data belonging to said data set of 1, and the random-number data generated with said random-number data generating transmitting means, to perform predetermined data conversion, and to generate the data for verification including a random-number data generating transmitting means transmit the random-number data which were generated and said data-conversion means made generate random-number data to said sending set.
[Claim 9] By transmitting the data for an encryption communication link with which the data for a communication link were enciphered to a receiving set from a sending set, and decrypting before cryptocommunication, the data for an encryption communication link which the receiving set received using the key data for decode which self holds A receiving set shares the data for a communication link which a sending set memorizes beforehand, and this actuation is followed. The 2nd address data with the 1st address which are the sending sets in the device authentication system which performs cryptocommunication using the shared data for a communication link, and can specify the 2nd address data from the 1st address data, A set storage means to memorize beforehand two or more data for the encryption communication link with the 2nd address which can specify the data for an encryption communication link from the 2nd address data, respectively, A 1st address-data receiving means to receive the 1st address data from said receiving set, From two or more 2nd address data with the 1st address memorized by said set storage means A 2nd address-data extract means to extract the 2nd address data specified with the 1st address data received by said 1st address-data receiving means from said receiving set, A data receiving means for verification to receive said data for the 1st verification from said receiving set, It carries out based on the 2nd address data extracted by said 2nd address-data extract means. A data-conversion means to perform predetermined data conversion and to generate the data for the 2nd verification, A verification means by which the data for the 1st verification received

by said data receiving means for verification and the data for the 2nd verification generated by said data-conversion means verify whether it is the same value, When it is verified by said verification means that it is the same value, from two or more data for the encryption communication link with the 2nd address memorized beforehand A data extraction means for an encryption communication link to extract the data for an encryption communication link specified with the 2nd address data extracted by said 2nd address-data extract means, The sending set characterized by having a data transmitting means for an encryption communication link to transmit the data for an encryption communication link extracted by said data extraction means for an encryption communication link to said receiving set.

[Claim 10] Said data-conversion means includes a random-number data generating transmitting means to transmit the random-number data which were made to generate random-number data and were generated to said receiving set. Said data-conversion means The sending set according to claim 9 which carries out based on the 2nd address data extracted by said 2nd address-data extract means, and the random-number data generated with said random-number data generating transmitting means, and is characterized by performing predetermined data conversion and generating the data for the 2nd verification.

[Claim 11] Said data-conversion means is a sending set according to claim 9 characterized by carrying out based on the 2nd address data extracted by said 2nd address-data extract means, and the random-number data received by said random-number data receiving means, performing predetermined data conversion, and generating the data for the 2nd verification including a random-number data receiving means by which said data-conversion means receives random-number data from said receiving set.

[Claim 12] By transmitting the data for an encryption communication link with which the data for a communication link were enciphered to a receiving set from a sending set, and decrypting before cryptocommunication, the data for an encryption communication link which the receiving set received using the key data for decode which self holds A receiving set shares the data for a communication link which a sending set memorizes beforehand, and this actuation is followed. It is the record medium which recorded the program by the side of the receiving set in the device authentication system which performs cryptocommunication using the shared data for a communication link and in which computer reading is possible. Said receiving set One sets or more of data sets which consist of the 1st address data, the 2nd address data, and key data for decode are memorized beforehand. The 1st address-data transmitting step which transmits to a computer the 1st address data with which said receiving set belongs to the data set of one of the data sets memorized beforehand to said sending set, Carry out based on the 2nd address data belonging to said data set of 1, and predetermined data conversion is performed. The data-conversion step which generates the data for verification, and the data transmitting step for

verification which transmits said data for verification to said sending set, The data receiving step for an encryption communication link which receives the data for an encryption communication link from said sending set, The data for an encryption communication link received by said data receiving step for an encryption communication link The record medium which recorded the program by the side of the receiving set characterized by performing the decryption step which decrypts using the key data for decode belonging to said data set of 1, and generates the data for a communication link and in which computer reading is possible.

[Claim 13] By transmitting the data for encryption authentication with which the data for authentication were enciphered to a receiving set from a sending set, and decrypting before cryptocommunication, the data for encryption authentication which the receiving set received using the key data for decode which self holds A receiving set shares the data for authentication which a sending set memorizes beforehand, and this actuation is followed. It is the record medium which recorded the program by the side of the sending set in the device authentication system which performs cryptocommunication using the shared data for authentication and in which computer reading is possible. Said sending set The 2nd address data with the 1st address which can specify the 2nd address data from the 1st address data, The data for the encryption communication link with the 2nd address which can specify the data for an encryption communication link from the 2nd address data The 1st address-data receiving step which has memorized more than one beforehand, respectively and receives the 1st address data from said receiving set to a computer, Said receiving set from two or more 2nd address data with the 1st address memorized beforehand The 2nd address-data extract step which extracts the 2nd address data specified with the 1st address data received by said 1st address-data receiving step from said receiving set, The data receiving step for verification which receives said data for the 1st verification from said receiving set, It carries out based on the 2nd address data extracted by said 2nd address-data extract step. The data-conversion step which performs predetermined data conversion and generates the data for the 2nd verification, The verification step to which the data for the 1st verification received by said data receiving step for verification and the data for the 2nd verification generated by said data-conversion step verify whether it is the same value, When it is verified by said verification step that it is the same value, from two or more data for the encryption communication link with the 2nd address memorized beforehand The data extraction step for an encryption communication link which extracts the data for an encryption communication link specified with the 2nd address data extracted by said 2nd address-data extract step, The record medium which recorded the program by the side of the sending set characterized by making it perform with the data transmitting step for an encryption communication link which transmits the data for an encryption communication link extracted by said data extraction step for an encryption communication link to said receiving set and in which computer reading is

possible.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] About the equipment which performs an encryption communication link, this invention relates to a device authentication technique for the equipment of a communications partner to confirm whether it is the right, before starting a communication link especially.
[0002]
[Description of the Prior Art] Plaintext data are acquired by the equipment of a transmitting side enciphering plaintext data using an encryption key, transmitting through a channel, and the equipment of a receiving side receiving this, and generally, decrypting in an encryption communication link, using a decode key. Thus, since only the enciphered data will be sent out to a channel, it knows [plaintext data] and is safe even if the data on a channel are monitored by the third party. It is SECURE about the channel which transmits and receives the enciphered data here. AUTHENTICATED It is referred to as CHANNEL.
[0003] Moreover, the equipment of a transmitting side is SECURE about it being the right receiver in which the equipment of a receiving side had a suitable decode key. AUTHENTICATED Device authentication processing which takes the initiative for opening CHANNEL and is checked is carried out widely. On the other hand, since digitized voice data, such as music, can do the completely same thing as an original copy if they are copied, its demand of making it want to be easily copied from a viewpoint of protection of copyrights is strong. Then, the memory card which surely enciphers and outputs the digitized voice data currently recorded appeared. This memory card performs the audio equipment and mutual recognition for playback, and transmits the digitized voice data enciphered to the audio equipment attested with it being a right receiver using the common key data generated in process of mutual recognition.
[0004] Drawing 3 is drawing showing the encryption communication system for explaining the outline of the device authentication processing in the conventional encryption communication link. The encryption communication system shown in drawing 3 consists of a player 900 and key media 950. It shall be the audio equipment which can receive the digitized voice data enciphered as the player here, and can reproduce voice, and shall be the memory stick equipped with the function which enciphers the digitized voice data currently recorded as key media, and is transmitted

etc.
[0005] A player 900 is equipped with the authentication demand section 901, the encryption data set receive section 902, the data set storage section 903, the data set selection section 904, the encryption data extraction section 905, the decryption section 906, the mutual recognition section 907, the encryption voice data receive section 908, and the voice playback section 909. The authentication demand section 901 requires device authentication of the key media 950.
[0006] The encryption data set receive section 902 receives the encryption data set with the address from the key media 950 after a demand of the device authentication by the authentication demand section 901. The encryption data set with the address is the encryption data aggregate which enciphered the common plaintext data memorized beforehand using various key data with the common encryption means to the key media 950, and was obtained here, the address is attached to each encryption data and encryption data can be specified from the data of this address. Here, one encryption data is 8 bytes and the encryption data set with the address is taken as the encryption data aggregate with the address of a 16 line x512 train (8K) individual.
[0007] The data set storage section 903 has memorized beforehand one sets or more of data sets which consist of address data and key data. The encryption data with which the address which the address data in the data set which it is here show was in agreement with which the address in the encryption data set with the address which receives in the encryption data set receive section 902 with data, and this address was added were enciphered using the key data in this data set. Here, 16 data sets are memorized beforehand.
[0008] The data set selection section 904 chooses one set as arbitration from the data sets one sets or more beforehand memorized by the data set storage section 903. The encryption data extraction section 905 extracts the encryption data specified with the address data in the data set chosen by the data set selection section 904 from the encryption data set with the address received by the encryption data set receive section 902.
[0009] The decryption section 906 decrypts the encryption data extracted by the encryption data extraction section 905 using the key data in the data set chosen by the data set selection section 904, generates plaintext data, decrypts the encryption voice data received from the key media 950 using the share key which the mutual recognition section 907 generates further, and generates voice data.
[0010] The mutual recognition section 907 performs mutually mutual recognition processing which carries out device authentication between a player and key media, using the plaintext data decrypted by the decryption section 906 and the 1st random-number data received from the key media 950, on the other hand, tropism conversion is performed, and generates the data for player authentication in which it is shown to the key media 950 that predetermined self is [which was defined beforehand] a right receiver, and transmits. Moreover, the 1st random-number data are generated

themselves, it transmits to the key media 950, and the data for key media authentication in which it is shown that the key media 950 are right transmitters are received, and when in agreement with said data for key media authentication which generated by performing tropism conversion on the other hand using said plaintext data and 1st random-number data generated themselves, it attests with it being a right transmitter. Furthermore, the share key used in order to decrypt the encryption voice data received from the key media 950 is generated.

[0011] A share key generates by performing the aforementioned one direction nature conversion here using the addition random-number data which carried out the exclusive OR of the received 1st random-number data and the 2nd random-number data generated themselves, and said plaintext data. Moreover, encryption voice data is transmitted only when the key media 950 attest the player 900 concerned with it being a right receiver.

[0012] The encryption voice data receive section 908 receives encryption voice data from the key media 950. The voice playback section 909 reproduces voice using the voice data which was decrypted by the decryption section 906 and generated. The key media 950 are equipped with the plaintext data storage section 951, the authentication demand reception section 952, the encryption data set storage section 953, the encryption data set transmitting section 954, the mutual recognition section 955, the voice data Records Department 956, the encryption section 957, and the encryption voice data transmitting section 958.

[0013] The plaintext data storage section 951 memorizes one predetermined plaintext data beforehand. Here, 7 bytes of one plaintext data is memorized beforehand. The authentication demand reception section 952 receives an authentication demand from a player 900. The encryption data set storage section 953 memorizes the encryption data set with the address beforehand. Here, the encryption data set with the address considers as the encryption data aggregate with the address of a 16 line x512 train (8K) individual, and one encryption data is made into 8 bytes.

[0014] The encryption data set transmitting section 954 returns the encryption data set memorized by the encryption data set storage section 952, when an authentication demand is received by the authentication demand reception section 951. The mutual recognition section 955 performs mutual recognition processing with the mutual recognition section 907, generates the 2nd random-number data itself, transmits to a player 900, and receives the data for player authentication. When in agreement with the same data for player authentication as the mutual recognition section 907 which generated by performing tropism conversion on the other hand using the plaintext data memorized by the plaintext data storage section 951 and the 2nd random-number data generated themselves, it attests with it being a right receiver. Moreover, using said plaintext data and the 2nd random-number data received from a player 900, the aforementioned one direction nature conversion is performed, and the data for key media authentication are generated and it transmits.

Furthermore, the share key used in order to encipher the voice data recorded on the voice data Records Department 956 to the encryption voice data transmitted to a player 900 is generated.

[0015] A share key generates by performing the aforementioned one direction nature conversion here using the addition random-number data which carried out the exclusive OR of the 1st random-number data generated themselves and the received 2nd random-number data, and said plaintext data. The voice data Records Department 956 records voice data. When attested with a player 900 being a right receiver by the mutual recognition section 955, the encryption section 957 enciphers the voice data recorded on the voice data Records Department 956 using the share key generated by the mutual recognition section 955, and generates encryption voice data.

[0016] The encryption voice data transmitting section 958 transmits the encryption voice data generated by the encryption section 957 to a player 900. Here, sharing of the plaintext data in the conventional encryption communication link, mutual recognition processing, generation of a share key, transmission and reception of encryption voice data, and actuation of audio playback are explained.

(1) The authentication demand section 901 of a player 900 requires device authentication of the key media 950.

(2) The authentication demand reception section 951 of the key media 950 receives a demand of device authentication.

(3) If the key media 950 receive a demand of device authentication, the encryption data set transmitting section 953 of the key media 950 will return the encryption data set memorized by the encryption data set storage section 952.

(4) The encryption data set receive section 902 of a player 900 receives the returned encryption data set with the address.

(5) The data set selection section 904 of a player 900 chooses one set as arbitration from the data sets beforehand memorized by the data set storage section 903.

(6) The encryption data extraction section 905 of a player 900 extracts the encryption data specified with the address data in the data set chosen by the data set selection section 904 from the encryption data set with the address received by the encryption data set receive section 902.

(7) The decryption section 906 of a player 900 decrypts the encryption data extracted by the encryption data extraction section 905 using the key data in the data set concerned, and generates plaintext data.

(8) The mutual recognition section 955 of the key media 950 generates the 1st random-number data, and transmits to a player 900.

(9) predetermined [which the mutual recognition section 907 of a player 900 defined beforehand using the plaintext data which received the 1st random-number data from the key media 950, and were decrypted by the decryption section 906, and the received 1st random-number data] -- on the other hand, perform tropism conversion,

generate the data for player authentication, transmit to the key media 950, generate the 2nd random-number data and transmit to the key media 950.
(10) Receive the data for player authentication, and using said plaintext data and 1st random-number data generated themselves, on the other hand, perform tropism conversion, and generate the data for player authentication, and the mutual recognition section 955 of the key media 950 attests with a player 900 being a right receiver, when [said] both are in agreement. Processing is stopped when not in agreement.
(11) If attested with a player 900 being a right receiver, the mutual recognition section 955 of the key media 950 will receive the 2nd random-number data from a player 900. The plaintext data memorized by the plaintext data storage section 951 and the received 2nd random-number data are used. The aforementioned one direction nature conversion is performed using the addition random-number data which carried out the exclusive OR of said 1st random-number data which performed tropism conversion on the other hand, generated the data for key media authentication, transmitted to the player 900, and were generated themselves, and the received 2nd random-number data, and said plaintext data, and a share key is generated.
(12) Receive the data for key media authentication, and using said plaintext data and 2nd random-number data generated themselves, on the other hand, perform tropism conversion, and generate the data for key media authentication, and the mutual recognition section 907 of a player 900 attests with the key media 950 being right transmitters, when [said] both are in agreement. Processing is stopped when not in agreement.
(13) If attested with the key media 950 being right transmitters, the mutual recognition section 907 of a player 900 will perform the aforementioned one direction nature conversion using the addition random-number data which carried out the exclusive OR of the received 1st random-number data and the 2nd random-number data generated themselves, and said plaintext data, and will generate a share key.
(14) The encryption section 957 of the key media 950 enciphers the voice data recorded on the voice data Records Department 956 using the share key generated by the mutual recognition section 955, and generates encryption voice data.
(15) The encryption voice data transmitting section 958 of the key media 950 transmits the encryption voice data generated by the encryption section 957 to a player 900.
(16) The encryption voice data receive section 908 of a player 900 receives encryption voice data from the key media 950.
(17) The decryption section 906 of a player 900 decrypts the encryption voice data received from the key media 950 using the share key generated by the mutual recognition section 907, and generates voice data.
(18) The voice playback section 909 of a player 900 reproduces voice using the voice data which was decrypted by the decryption section 906 and generated.

[0017] As mentioned above, the conventional encryption communication system is equipped with the structure that key media permit the output of the data with which a player is recognized to be a right receiver and key media are recording it when the player holds at least one or more suitable key data. In the still more above conventional encryption communication system, key media have the function which eliminates the player considered that is inaccurate by a certain reason. It can be made accuracy by the ability not using the key media manufactured or put on the market after considering that it is inaccurate in the player considered that is inaccurate.
[0018] In the time of sale, K effective encryption 8 data with the address shall be altogether memorized by the encryption data set storage section 953 of the key media 950, for example. 16 data sets are memorized by the data set storage section 903 of a player 900, and it corresponds for any of the 8K pieces of the encryption data set storage section 953 of the key media 950 being, respectively, and has become the combination which changes with the manufacturers and models of player.
[0019] By a certain reason, if it is considered that a certain player is inaccurate, the encryption data corresponding to 16 data sets memorized by the data set storage section 903 of the player considered that is inaccurate will be altogether placed and changed into invalid data here in the encryption data set memorized by the encryption data set storage section 953 of the key media 950 manufactured or put on the market after it.
[0020] Since all the data sets memorized by the data set storage section of the player considered that is inaccurate by carrying out like this become an invalid, it becomes impossible for the player considered that is inaccurate to read data from the key media. In addition, since data can be read from key media if other players have [at least one] 16 effective data sets, it can respond to the player of other types.
[0021]
[Problem(s) to be Solved by the Invention] After having stored the plaintext data acquired justly and considering that it is inaccurate before considering that the player which it is here is inaccurate, the data address of the suitable key data which he does not hold is transmitted to key media, encryption data are obtained, and this player becomes a right receiver and can clear up by advancing processing after using the plaintext data stored beforehand, without decrypting this encryption data.
[0022] The structure that key media permit the output of the data with which a player is recognized to be a right receiver and key media are recording it when the player holds suitable key data since it has an illusion that it is a right receiver, in the player although the player will not hold the key data corresponding to the data address to which key media were transmitted from the player, if a player performs such processing stops functioning proper.
[0023] Then, even if it stores plaintext data before it is considered that the receiving set of this invention is inaccurate, it aims at offering the device authentication system

which can eliminate the receiving set considered that is inaccurate, a sending set, receiving sets, those approaches, and the record medium that recorded those programs.

[0024]

[Means for Solving the Problem] In order to attain the above-mentioned object, the device authentication approach concerning this invention The data for an encryption communication link with which the data for a communication link were enciphered are transmitted to a receiving set from a sending set before cryptocommunication. A receiving set shares the data for a communication link which a sending set memorizes beforehand by decrypting the data for an encryption communication link which the receiving set received using the key data for double signs which self holds. It is the device authentication approach in the cryptocommunication system which performs cryptocommunication using the data for a communication link shared following on this actuation. Said receiving set has memorized beforehand one sets or more of data sets which consist of the 1st address data, the 2nd address data, and key data for decode. The 2nd address data with the 1st address with which said sending set can specify the 2nd address data from the 1st address data, Two or more data for the encryption communication link with the 2nd address which can specify the data for an encryption communication link from the 2nd address data are memorized beforehand, respectively. The 1st address-data transmission step which transmits the 1st address data with which said receiving set belongs to the data set of one of the data sets memorized beforehand to said sending set from said receiving set, The 2nd address-data extract step which extracts the 2nd address data specified with the 1st address data transmitted by said 1st address-data transmission step from said receiving set from two or more 2nd address data with the 1st address beforehand memorized in said sending set, The verification step to which the 2nd address data belonging to said data set of 1 in said receiving set and the 2nd address data extracted by said 2nd address-data extract step in said sending set verify whether it is the same value, When it is verified by said verification step that it is the same value, it sets to said sending set. The data extraction step for an encryption communication link which extracts the data for an encryption communication link specified with the 2nd address data extracted from two or more data for the encryption communication link with the 2nd address memorized beforehand by said 2nd address-data extract step, The data transmission step for an encryption communication link which transmits the data for an encryption communication link extracted by said data extraction step for an encryption communication link to said receiving set from said sending set, It is characterized by having the decryption step which decrypts the data for an encryption communication link transmitted by said data transmission step for an encryption communication link in said receiving set using the key data for decode belonging to said data set of 1, and generates the data for a communication link.

[0025] In order to attain the above-mentioned object, the device authentication

system concerning this invention The data for an encryption communication link with which the data for a communication link were enciphered are transmitted to a receiving set from a sending set before cryptocommunication. A receiving set shares the data for a communication link which a sending set memorizes beforehand by decrypting the data for an encryption communication link which the receiving set received using the key data for decode which self holds. It is the device authentication system which consists of a sending set which performs cryptocommunication using the data for a communication link shared following on this actuation, and a receiving set. Said receiving set A data set storage means to memorize beforehand one sets or more of data sets which consist of the 1st address data, the 2nd address data, and key data for decode, A 1st address-data transmitting means to transmit the 1st address data belonging to the data set of one of the data sets memorized by said data set storage means to said sending set, Carry out based on the 2nd address data belonging to said data set of 1, and predetermined data conversion is performed. A 1st data-conversion means to generate the data for the 1st verification, and a data transmitting means for the 1st verification to transmit said data for the 1st verification to said sending set, A data receiving means for an encryption communication link to receive the data for an encryption communication link from said sending set, It has a decryption means to decrypt the data for an encryption communication link received by said data receiving means for an encryption communication link using the key data for decode belonging to said data set of 1, and to generate the data for a communication link. A set storage means to memorize beforehand two or more data for the encryption communication link with the 2nd address which can specify the data for an encryption communication link, respectively from the 2nd address data with the 1st address with which said sending set can specify the 2nd address data from the 1st address data, and the 2nd address data, A 1st address-data receiving means to receive the 1st address data from said receiving set, A 2nd address-data extract means to extract the 2nd address data specified with the 1st address data received by said 1st address-data receiving means from said receiving set from two or more 2nd address data with the 1st address memorized by said set storage means, A data receiving means for the 1st verification to receive said data for the 1st verification from said receiving set, A 2nd data-conversion means to carry out based on the 2nd address data extracted by said 2nd address-data extract means, to perform the same data conversion as said 1st data-conversion means, and to generate the data for the 2nd verification, A verification means by which the data for the 1st verification received by said data receiving means for the 1st verification and the data for the 2nd verification generated by said 2nd data-conversion means verify whether it is the same value, With said 2nd address-data extract means from two or more data for the encryption communication link with the 2nd address beforehand memorized when it is verified by said verification means that it is the same value A data extraction means for an

encryption communication link to extract the data for an encryption communication link specified with the 2nd extracted address data, It is characterized by having a data transmitting means for an encryption communication link to transmit the data for an encryption communication link extracted by said data extraction means for an encryption communication link to said receiving set.

[0026]

[Embodiment of the Invention] As for <outline> this invention, a sending set memorizes beforehand the escape address-data set with the address, and the encryption data set with the extended address. One sets or more of data sets which a receiving set (player) becomes from address data, extended address data, and key data are memorized beforehand. Before making the address of encryption data into indirection reference and beginning cryptocommunication, a sending set (key media) After verifying that a receiving set is just using extended address data, It is the encryption communication system which transmits only these extended address data and corresponding encryption data to a receiving set, without transmitting and receiving all encryption data sets like the former. Plaintext data are shared between encryption data being decrypted with a receiving set and becoming plaintext data, and cryptocommunication is performed using this plaintext data.

[0027] <Configuration> drawing 1 is drawing showing the configuration of the encryption communication system concerning the gestalt of this operation. The encryption communication system shown in drawing 1 consists of a player 100 and key media 150. A player 100 is the audio equipment which can receive the enciphered digitized voice data and can reproduce voice, and is a thing which has it verified by the key media 150 whether it is a just receiver before the encryption data which become the origin of the plaintext data used for cryptocommunication are transmitted. The data set storage section 101, the data set selection section 102, the address-data transmitting section 103, the random-number data receive section 104, the one direction nature converter 105, the data transmitting section 106 for verification, the encryption data receive section 107, the decryption section 108, the mutual recognition section 907, the encryption voice data receive section 908, And it has the voice playback section 909.

[0028] It is what verifies whether the key media 150 are the memory sticks equipped with the function which enciphers the digitized voice data currently recorded and is transmitted etc., and they are receivers with a just player 100 before they transmit encryption data. The plaintext data storage section 951, the extended address-data set storage section 151, the address-data receive section 152, the extended address-data extract section 153, the random-number data generating section 154, the random-number data transmitting section 155, the one direction nature converter 156, the data receive section 157 for verification, the verification section 158, It has the encryption data set storage section 159, the encryption data extraction section 160, the encryption data transmitting section 161, the mutual recognition section 955,

the voice data Records Department 956, the encryption section 957, and the encryption voice data transmitting section 958. The component shown by the number same here as the component in the conventional encryption communication system abbreviates explanation of Perilla frutescens (L.) Britton var. crispa (Thunb.) Decne. to what has the same function.

[0029] The data set storage section 101 has memorized beforehand one sets or more of data sets which consist of address data, extended address data, and key data. Here, 16 data sets are memorized beforehand. The data set selection section 102 chooses an one-set data set as arbitration from the data sets one sets or more beforehand memorized by the data set storage section 101.

[0030] The address-data transmitting section 103 transmits the address data in the data set chosen by the data set selection section 102 to the key media 150. The random-number data receive section 104 receives random-number data from the key media 150. On the other hand, on the other hand, the tropism converter 105 performs tropism conversion using the extended address data in the data set chosen by the data set selection section 102, and the random-number data received by the random-number data receive section 104, and generates the data for verification.

[0031] The data transmitting section 106 for verification transmits the data for verification which the tropism converter 105 generated on the other hand to the key media 150. The encryption data receive section 107 receives encryption data from the key media 150. Here, 8 bytes of one encryption data is received. The decryption section 108 decrypts the encryption data received by the encryption data receive section 107 using the key data in the data set chosen by the data set selection section 102, generates plaintext data, decrypts the encryption voice data received from the key media 150 using the share key which the mutual recognition section 907 generates further, and generates voice data.

[0032] The extended address-data set storage section 151 memorizes the escape address-data set with the address. The escape address-data set with the address is the data aggregate which shows the extended address under encryption data set with the extended address memorized by the encryption data set storage section 159 here, the address is attached to each extended address data, and extended address data can be specified from the data of this address. Here, the escape address-data set with the address is taken as the set of the escape address data with the address of a 16 line x512 train (8K) individual.

[0033] The address-data receive section 152 receives address data from a player 100. The extended address-data extract section 153 extracts the extended address data with which the address which the address data received by the address-data receive section 152 show was added from the escape address-data set with the address memorized by the extended address-data set storage section 151.

[0034] The random-number data generating section 154 generates random-number data. The random-number data transmitting section 155 transmits the random-

number data which the random-number data generating section 154 generated to a player 100. On the other hand, on the other hand, the tropism converter 156 performs tropism conversion using the extended address data extracted by the extended address-data extract section 153 and the random-number data generated by the random-number data generating section 154, and generates the data for verification.
[0035] The data receive section 157 for verification receives the data for verification from a player 100. The verification section 158 verifies whether the data for verification generated by the tropism converter 156 on the other hand and the data for verification received by the data receive section 157 for verification are the same values. The encryption data set storage section 159 memorizes the encryption data set with the extended address. The encryption data set with the extended address is the encryption data aggregate which enciphered the common plaintext data memorized beforehand using various key data with the common encryption means in the plaintext data storage section 951 of the key media 150, and was obtained here, the extended address is attached to each encryption data, and encryption data can be specified from the data of this extended address. Here, one encryption data is 8 bytes and the encryption data set with the extended address is taken as the encryption data aggregate with the extended address of a 16 line x512 train (8K) individual.
[0036] The encryption data extraction section 160 extracts the encryption data specified with the extended address data extracted by the extended address-data extract section 153 from the encryption data set with the extended address memorized by the encryption data set storage section 159, when the data for verification are the same value. The encryption data transmitting section 161 transmits the encryption data extracted by the encryption data extraction section 160 to a player 100. Here, 8 bytes of one encryption data is transmitted.
[0037] <Actuation> Here, sharing of the plaintext data in the encryption communication link of the gestalt of this operation, mutual recognition processing, generation of a share key, transmission and reception of encryption voice data, and actuation of audio playback are explained. Drawing 2 is drawing showing an example of actuation of the encryption communication system of the gestalt of this operation.
(1) The data set selection section 102 of a player 100 chooses an one-set data set as arbitration from the data sets one sets or more beforehand memorized by the data set storage section 101 (step S1).
(2) The address-data transmitting section 103 of a player 100 transmits the address data in the data set chosen by the data set selection section 102 to the key media 150 (step S2).
(3) The address-data receive section 152 of the key media 150 receives address data from a player 100 (step S3).
(4) The extended address-data extract section 153 of the key media 150 extracts the extended address data specified with the address data received by the address-data

receive section 152 from the escape address-data set with the address memorized by the extended address-data set storage section 151 (step S4).
(5) The random-number data generating section 154 of the key media 150 generates random-number data (step S5).
(6) The random-number data transmitting section 155 of the key media 150 transmits the random-number data which the random-number data generating section 154 generated to a player 100 (step S6).
(7) The random-number data receive section 104 of a player 100 receives random-number data from the key media 150 (step S7).
(8) On the other hand, on the other hand, the tropism converter 105 performs tropism conversion using the extended address data in the data set of a player 100 chosen by the data set selection section 102, and the random-number data received by the random-number data receive section 104, and generates the data for verification (step S8).
(9) The data transmitting section 106 for verification of a player 100 transmits the data for verification which the tropism converter 105 generated on the other hand to the key media 150 (step S9).
(10) On the other hand, perform tropism conversion using the escape address data of the key media 150 from which the tropism converter 156 was extracted by the extended address-data extract section 153 on the other hand, and the random-number data generated by the random-number data generating section 154, and generate the data for verification (step S10).
(11) The verification section 158 of the key media 150 verifies whether the data for verification generated by the tropism converter 156 on the other hand and the data for verification received by the data receive section 157 for verification are the same values (step S11). Future processings are stopped when it is not the same value.
(12) When the data for verification are the same value, the encryption data extraction section 160 of the key media 150 extracts the encryption data specified with the extended address data extracted by the extended address-data extract section 153 from the encryption data set with the extended address memorized by the encryption data set storage section 159 (step S12).
(13) The encryption data transmitting section 161 of the key media 150 transmits the encryption data extracted by the encryption data extraction section 160 to a player 100 (step S13).
(14) The encryption data receive section 107 of a player 100 receives encryption data from the key media 150 (step S14).
(15) The decryption section 108 of a player 100 decrypts the encryption data received by the encryption data receive section 107 using the key data in the data set chosen by the data set selection section 102, and generates plaintext data (step S15).
[0038] Sharing of plaintext data was completed even here. Generation of the mutual

recognition processing and the share key which are explained below, transmission and reception of encryption voice data, and actuation (step S16) of audio playback are the same as that of what was explained by the Prior art.
(16) The mutual recognition section 955 of the key media 150 generates the 1st random-number data, and transmits to a player 900.
(17) predetermined [which the mutual recognition section 907 of a player 100 defined beforehand using the plaintext data which received the 1st random-number data from the key media 150, and were decrypted by the decryption section 108, and the received 1st random-number data] -- on the other hand, perform tropism conversion, generate the data for player authentication, transmit to the key media 150, generate the 2nd random-number data and transmit to the key media 150.
(18) Receive the data for player authentication, and using said plaintext data and 1st random-number data generated themselves, on the other hand, perform tropism conversion, and generate the data for player authentication, and the mutual recognition section 955 of the key media 150 attests with a player 100 being a right receiver, when [said] both are in agreement. Processing is stopped when not in agreement.
(19) If attested with a player 100 being a right receiver, the mutual recognition section 955 of the key media 150 will receive the 2nd random-number data from a player 100. The plaintext data memorized by the plaintext data storage section 951 and the received 2nd random-number data are used. The aforementioned one direction nature conversion is performed using the addition random-number data which carried out the exclusive OR of said 1st random-number data which performed tropism conversion on the other hand, generated the data for key media authentication, transmitted to the player 100, and were generated themselves, and the received 2nd random-number data, and said plaintext data, and a share key is generated.
(20) Receive the data for key media authentication, and using said plaintext data and 2nd random-number data generated themselves, on the other hand, perform tropism conversion, and generate the data for key media authentication, and the mutual recognition section 907 of a player 100 attests with the key media 950 being right transmitters, when [said] both are in agreement. Processing is stopped when not in agreement.
(21) If attested with the key media 150 being right transmitters, the mutual recognition section 907 of a player 100 will perform the aforementioned one direction nature conversion using the addition random-number data which carried out the exclusive OR of the received 1st random-number data and the 2nd random-number data generated themselves, and said plaintext data, and will generate a share key.
(22) The encryption section 957 of the key media 150 enciphers the voice data recorded on the voice data Records Department 956 using the share key generated by the mutual recognition section 955, and generates encryption voice data.
(23) The encryption voice data transmitting section 958 of the key media 150

transmits the encryption voice data generated by the encryption section 957 to a player 100.
(24) The encryption voice data receive section 908 of a player 100 receives encryption voice data from the key media 150.
(25) The decryption section 108 of a player 100 decrypts the encryption voice data received from the key media 150 using the share key generated by the mutual recognition section 907, and generates voice data.
(26) The voice playback section 909 of a player 100 reproduces voice using the voice data which was decrypted by the decryption section 108 and generated.
[0039] As mentioned above, according to the encryption communication system of the gestalt of this operation, a player 100 can obtain encryption data, only when the extended address data corresponding to the address data transmitted to the key media 150 are held. Even if a player 100 transmits the suitable address data which he does not hold to the key media 150, it cannot obtain encryption data, but it becomes a right receiver and it becomes impossible therefore, to clear up them.
[0040] In addition, with the gestalt of this operation, although the key media 150 were equipped with the random-number data generating section and the random-number data generating section, a player 100 may be equipped with these. What is necessary is just to be able to share the same random-number data by transmitting the random-number data which were made to generate random-number data and were generated within a player 100 or the key media 150 in short to another side. Moreover, while the tropism converter 156 carries out on the other hand with the tropism converter 105, tropism conversion does not necessarily need to use random-number data. Moreover, on the other hand, data conversion performed here may not necessarily be tropism conversion, and as long as these two converters perform the same data conversion, it may be anything. However, if tropism conversion is performed on the other hand using random-number data like the gestalt of this operation, even if the extended address data by which data conversion was carried out are monitored by the third party on a channel, risk of extended address data being known is very low safe.
[0041] Moreover, since it is contained in the random-number data generating section, the mutual recognition section 907 of the former [on the other hand / converter / tropism] from the first, or the mutual recognition section 955 and can use with these in common, there are few additions of hardware and software, and it ends. Moreover, with the gestalt of this operation, although the encryption data set storage section 159 memorized the encryption data set with the extended address, the encryption data set with the address may be memorized. In such a case, the encryption data extraction section 160 extracts the encryption data specified with the address data received by the address-data receive section 152 from the encryption data set with the address memorized by the encryption data set storage section 159.
[0042] Moreover, although the gestalt of this operation made the example audio equipment, etc. a memory stick, etc. which can reproduce voice and explained them, it

may be adapted for what kind of equipment which performs an encryption communication link. For example, a certain data may be transmitted and received between personal computers through communication lines, such as the Internet. Moreover, the program which can make a computer perform actuation like the gestalt of this operation is recorded on the record medium in which computer reading is possible, this record medium circulates, and it can be set as the object of dealings.
[0043] The record media in which computer reading is possible are fixed record media, such as removable record media, such as for example, a floppy (trademark) disk, CD, MO and DVD, and memory card, and a hard disk, and semiconductor memory, etc., and it is not limited especially here.
[0044]
[Effect of the Invention] The device authentication approach concerning this invention transmits before cryptocommunication the data for an encryption communication link with which the data for a communication link were enciphered to a receiving set from a sending set. A receiving set shares the data for a communication link which a sending set memorizes beforehand by decrypting the data for an encryption communication link which the receiving set received using the key data for double signs which self holds. It is the device authentication approach in the cryptocommunication system which performs cryptocommunication using the data for a communication link shared following on this actuation. Said receiving set has memorized beforehand one sets or more of data sets which consist of the 1st address data, the 2nd address data, and key data for decode. The 2nd address data with the 1st address with which said sending set can specify the 2nd address data from the 1st address data, Two or more data for the encryption communication link with the 2nd address which can specify the data for an encryption communication link from the 2nd address data are memorized beforehand, respectively. The 1st address-data transmission step which transmits the 1st address data with which said receiving set belongs to the data set of one of the data sets memorized beforehand to said sending set from said receiving set, The 2nd address-data extract step which extracts the 2nd address data specified with the 1st address data transmitted by said 1st address-data transmission step from said receiving set from two or more 2nd address data with the 1st address beforehand memorized in said sending set, The verification step to which the 2nd address data belonging to said data set of 1 in said receiving set and the 2nd address data extracted by said 2nd address-data extract step in said sending set verify whether it is the same value, When it is verified by said verification step that it is the same value, it sets to said sending set. The data extraction step for an encryption communication link which extracts the data for an encryption communication link specified with the 2nd address data extracted from two or more data for the encryption communication link with the 2nd address memorized beforehand by said 2nd address-data extract step, The data transmission step for an encryption communication link which transmits the data for an encryption

communication link extracted by said data extraction step for an encryption communication link to said receiving set from said sending set, It is characterized by having the decryption step which decrypts the data for an encryption communication link transmitted by said data transmission step for an encryption communication link in said receiving set using the key data for decode belonging to said data set of 1, and generates the data for a communication link.

[0045] Only when the receiving set (player) holds the 2nd address data corresponding to the 1st address data transmitted to a sending set (key media) according to this approach, a sending set (key media) transmits encryption data, and a receiving set (player) can receive encryption data, can continue at this actuation, and can perform cryptocommunication. Even if it transmits the 1st suitable address data to a sending set (key media), it becomes a right receiver and it becomes impossible therefore, to clear up a receiving set (player), since cryptocommunication cannot be performed unless the set of the 1st just address data and the 2nd just address data is held.

[0046] The device authentication system concerning this invention transmits before cryptocommunication the data for an encryption communication link with which the data for a communication link were enciphered to a receiving set from a sending set. A receiving set shares the data for a communication link which a sending set memorizes beforehand by decrypting the data for an encryption communication link which the receiving set received using the key data for decode which self holds. It is the device authentication system which consists of a sending set which performs cryptocommunication using the data for a communication link shared following on this actuation, and a receiving set. Said receiving set A data set storage means to memorize beforehand one sets or more of data sets which consist of the 1st address data, the 2nd address data, and key data for decode, A 1st address-data transmitting means to transmit the 1st address data belonging to the data set of one of the data sets memorized by said data set storage means to said sending set, Carry out based on the 2nd address data belonging to said data set of 1, and predetermined data conversion is performed. A 1st data-conversion means to generate the data for the 1st verification, and a data transmitting means for the 1st verification to transmit said data for the 1st verification to said sending set, A data receiving means for an encryption communication link to receive the data for an encryption communication link from said sending set, It has a decryption means to decrypt the data for an encryption communication link received by said data receiving means for an encryption communication link using the key data for decode belonging to said data set of 1, and to generate the data for a communication link. A set storage means to memorize beforehand two or more data for the encryption communication link with the 2nd address which can specify the data for an encryption communication link, respectively from the 2nd address data with the 1st address with which said sending set can specify the 2nd address data from the 1st address data, and the 2nd address data, A 1st address-data receiving means to receive the 1st address data from said

receiving set, A 2nd address-data extract means to extract the 2nd address data specified with the 1st address data received by said 1st address-data receiving means from said receiving set from two or more 2nd address data with the 1st address memorized by said set storage means, A data receiving means for the 1st verification to receive said data for the 1st verification from said receiving set, A 2nd data-conversion means to carry out based on the 2nd address data extracted by said 2nd address-data extract means, to perform the same data conversion as said 1st data-conversion means, and to generate the data for the 2nd verification, A verification means by which the data for the 1st verification received by said data receiving means for the 1st verification and the data for the 2nd verification generated by said 2nd data-conversion means verify whether it is the same value, With said 2nd address-data extract means from two or more data for the encryption communication link with the 2nd address beforehand memorized when it is verified by said verification means that it is the same value A data extraction means for an encryption communication link to extract the data for an encryption communication link specified with the 2nd extracted address data, It is characterized by having a data transmitting means for an encryption communication link to transmit the data for an encryption communication link extracted by said data extraction means for an encryption communication link to said receiving set.

[0047] Only when the receiving set (player) holds the 2nd address data corresponding to the 1st address data transmitted to a sending set (key media) according to this configuration, a sending set (key media) transmits encryption data, and a receiving set (player) can receive encryption data, can continue at this actuation, and can perform cryptocommunication. Even if it transmits the 1st suitable address data to a sending set (key media), it becomes a right receiver and it becomes impossible therefore, to clear up a receiving set (player), since cryptocommunication cannot be performed unless the set of the 1st just address data and the 2nd just address data is held.

[0048] The receiving set concerning this invention transmits before cryptocommunication the data for an encryption communication link with which the data for a communication link were enciphered to a receiving set from a sending set. A receiving set shares the data for a communication link which a sending set memorizes beforehand by decrypting the data for an encryption communication link which the receiving set received using the key data for decode which self holds. It is a receiving set in the device authentication system which performs cryptocommunication using the data for a communication link shared following on this actuation. A data set storage means to memorize beforehand one sets or more of data sets which consist of the 1st address data, the 2nd address data, and key data for decode, A 1st address-data transmitting means to transmit the 1st address data belonging to the data set of one of the data sets memorized by said data set storage means to said sending set, A data-conversion means to carry out based on the 2nd address data belonging to said data set of 1, to perform predetermined data

conversion, and to generate the data for verification, A data transmitting means for verification to transmit said data for verification to said sending set, A data receiving means for an encryption communication link to receive the data for an encryption communication link from said sending set, It is characterized by having a decryption means to decrypt the data for an encryption communication link received by said data receiving means for an encryption communication link using the key data for decode belonging to said data set of 1, and to generate the data for a communication link.
[0049] Since according to this configuration a receiving set (player) can generate the data for verification based on the 2nd address data only when the 2nd address data corresponding to the 1st address data transmitted to a sending set (key media) are held, it becomes a right receiver and it becomes impossible to clear up. The sending set concerning this invention transmits before cryptocommunication the data for an encryption communication link with which the data for a communication link were enciphered to a receiving set from a sending set. A receiving set shares the data for a communication link which a sending set memorizes beforehand by decrypting the data for an encryption communication link which the receiving set received using the key data for decode which self holds. The 2nd address data with the 1st address which are the sending sets in the device authentication system which performs cryptocommunication using the data for a communication link shared following on this actuation, and can specify the 2nd address data from the 1st address data, A set storage means to memorize beforehand two or more data for the encryption communication link with the 2nd address which can specify the data for an encryption communication link from the 2nd address data, respectively, A 1st address-data receiving means to receive the 1st address data from said receiving set, A 2nd address-data extract means to extract the 2nd address data specified with the 1st address data received by said 1st address-data receiving means from said receiving set from two or more 2nd address data with the 1st address memorized by said set storage means, A data receiving means for verification to receive said data for the 1st verification from said receiving set, A data-conversion means to carry out based on the 2nd address data extracted by said 2nd address-data extract means, to perform predetermined data conversion, and to generate the data for the 2nd verification, A verification means by which the data for the 1st verification received by said data receiving means for verification and the data for the 2nd verification generated by said data-conversion means verify whether it is the same value, With said 2nd address-data extract means from two or more data for the encryption communication link with the 2nd address beforehand memorized when it is verified by said verification means that it is the same value A data extraction means for an encryption communication link to extract the data for an encryption communication link specified with the 2nd extracted address data, It is characterized by having a data transmitting means for an encryption communication link to transmit the data for an encryption communication link extracted by said data extraction means for an encryption

communication link to said receiving set.
[0050] According to this configuration, since a sending set (key media) does not perform cryptocommunication, the receiving set (player) which does not transmit the data for right verification since encryption data can be transmitted, it can continue at this actuation and cryptocommunication can be performed only when the data for right verification are received from a receiving set (player) is safe for it. The record medium which recorded the program by the side of the receiving set concerning this invention and in which computer reading is possible The data for an encryption communication link with which the data for a communication link were enciphered are transmitted to a receiving set from a sending set before cryptocommunication. A receiving set shares the data for a communication link which a sending set memorizes beforehand by decrypting the data for an encryption communication link which the receiving set received using the key data for decode which self holds. It is the record medium which recorded the program by the side of the receiving set in the device authentication system which performs cryptocommunication using the data for a communication link shared following on this actuation and in which computer reading is possible. Said receiving set has memorized beforehand one sets or more of data sets which consist of the 1st address data, the 2nd address data, and key data for decode. The 1st address-data transmitting step which transmits to a computer the 1st address data with which said receiving set belongs to the data set of one of the data sets memorized beforehand to said sending set, The data-conversion step which carries out based on the 2nd address data belonging to said data set of 1, performs predetermined data conversion, and generates the data for verification, The data transmitting step for verification which transmits said data for verification to said sending set, The data receiving step for an encryption communication link which receives the data for an encryption communication link from said sending set, It is characterized by performing the decryption step which decrypts the data for an encryption communication link received by said data receiving step for an encryption communication link using the key data for decode belonging to said data set of 1, and generates the data for a communication link.
[0051] Since according to this program a receiving set (player) can generate the data for verification based on the 2nd address data only when the 2nd address data corresponding to the 1st address data transmitted to a sending set (key media) are held, it becomes a right receiver and it becomes impossible to clear up. The record medium which recorded the program by the side of the sending set concerning this invention and in which computer reading is possible The data for encryption authentication with which the data for authentication were enciphered are transmitted to a receiving set from a sending set before cryptocommunication. A receiving set shares the data for authentication which a sending set memorizes beforehand by decrypting the data for encryption authentication which the receiving set received using the key data for decode which self holds. It is the record medium which

recorded the program by the side of the sending set in the device authentication system which performs cryptocommunication using the data for authentication shared following on this actuation and in which computer reading is possible. Said sending set has memorized beforehand two or more data for the encryption communication link with the 2nd address which can specify the data for an encryption communication link, respectively from the 2nd address data with the 1st address which can specify the 2nd address data from the 1st address data, and the 2nd address data. To a computer The 1st address-data receiving step which receives the 1st address data from said receiving set, The 2nd address-data extract step which extracts the 2nd address data as which said receiving set is specified with the 1st address data received by said 1st address-data receiving step from said receiving set from two or more 2nd address data with the 1st address memorized beforehand, The data receiving step for verification which receives said data for the 1st verification from said receiving set, The data-conversion step which carries out based on the 2nd address data extracted by said 2nd address-data extract step, performs predetermined data conversion, and generates the data for the 2nd verification, The verification step to which the data for the 1st verification received by said data receiving step for verification and the data for the 2nd verification generated by said data-conversion step verify whether it is the same value, By said 2nd address-data extract step from two or more data for the encryption communication link with the 2nd address beforehand memorized when it is verified by said verification step that it is the same value The data extraction step for an encryption communication link which extracts the data for an encryption communication link specified with the 2nd extracted address data, The record medium which recorded the program by the side of the sending set characterized by making it perform with the data transmitting step for an encryption communication link which transmits the data for an encryption communication link extracted by said data extraction step for an encryption communication link to said receiving set and in which computer reading is possible.

[0052] According to this program, since a sending set (key media) does not perform cryptocommunication, the receiving set (player) which does not transmit the data for right verification since encryption data can be transmitted, it can continue at this actuation and cryptocommunication can be performed only when the data for right verification are received from a receiving set (player) is safe for it. In the device authentication approach moreover, said verification step In the random-number data sharing substep which shares the same random-number data by transmitting the random-number data which were made to generate random-number data and were generated within said receiving set or said sending set to another side, and said receiving set The 1st data-conversion substep which performs predetermined data conversion to the 2nd address data belonging to said data set of 1, and said shared random-number data, and generates the data for the 1st verification, In the data transmission substep for the 1st verification which transmits said data for the 1st

verification to said sending set from said receiving set, and said sending set In the 2nd data-conversion substep which performs the data conversion same to the 2nd address data extracted by said 2nd address-data extract step, and said shared random-number data as said 1st data-conversion substep, and generates the data for the 2nd verification, and said sending set Said data for the 1st verification and said data for the 2nd verification can also be characterized by having the verification substep which verifies whether it is the same value.

[0053] In a device authentication system, moreover, said 1st data-conversion means with which said receiving set is equipped A random-number data receiving means to receive random-number data from said sending set is included. Said 1st data-conversion means Carry out based on the 2nd address data belonging to said data set of 1, and the random-number data received by said random-number data receiving means, perform predetermined data conversion, and the data for the 1st verification are generated. Said 2nd data-conversion means with which said sending set is equipped A random-number data generating transmitting means to transmit the random-number data which were made to generate random-number data and were generated to said receiving set is included. Said 2nd data-conversion means It can carry out based on the 2nd address data extracted by said 2nd address-data extract means, and the random-number data generated with said random-number data generating transmitting means, and can also be characterized by performing predetermined data conversion and generating the data for the 2nd verification. Again Said 1st data-conversion means with which said receiving set is equipped Said random-number data generating transmitting means to transmit the random-number data which were made to generate random-number data and were generated to said sending set is included. Said 1st data-conversion means Carry out based on the 2nd address data belonging to said data set of 1, and the random-number data generated with said random-number data generating transmitting means, perform predetermined data conversion, and the data for the 1st verification are generated. Said 2nd data-conversion means with which said sending set is equipped A random-number data receiving means to receive random-number data from said receiving set is included. Said 2nd data-conversion means It can carry out based on the 2nd address data extracted by said 2nd address-data extract means, and the random-number data received by said random-number data receiving means, and can also be characterized by performing predetermined data conversion and generating the data for the 2nd verification.

[0054] In a receiving set moreover, said data-conversion means A random-number data receiving means to receive random-number data from said sending set is included. Said data-conversion means It can carry out based on the 2nd address data belonging to said data set of 1, and the random-number data received by said random-number data receiving means, and can also be characterized by performing predetermined data conversion and generating the data for verification. Said data-

conversion means includes a random-number data generating transmitting means to transmit the random-number data which were made to generate random-number data and were generated to said sending set. Moreover, said data-conversion means It can carry out based on the 2nd address data belonging to said data set of 1, and the random-number data generated with said random-number data generating transmitting means, and can also be characterized by performing predetermined data conversion and generating the data for verification.

[0055] In a sending set moreover, said data-conversion means A random-number data generating transmitting means to transmit the random-number data which were made to generate random-number data and were generated to said receiving set is included. Said data-conversion means It can carry out based on the 2nd address data extracted by said 2nd address-data extract means, and the random-number data generated with said random-number data generating transmitting means, and can also be characterized by performing predetermined data conversion and generating the data for the 2nd verification. Moreover, said data-conversion means A random-number data receiving means to receive random-number data from said receiving set is included. Said data-conversion means It can carry out based on the 2nd address data extracted by said 2nd address-data extract means, and the random-number data received by said random-number data receiving means, and can also be characterized by performing predetermined data conversion and generating the data for the 2nd verification.

[0056] Since data conversion of the 2nd address data is carried out and they are transmitted by this using random-number data, it knows [the 2nd address data] and is safe even if the data on a channel are monitored by the third party.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the configuration of the encryption communication system concerning the gestalt of this operation.

[Drawing 2] It is drawing showing an example of actuation of the encryption communication system of the gestalt of this operation.

[Drawing 3] It is drawing showing the encryption communication system for explaining the outline of the device authentication processing in the conventional encryption communication link.

[Description of Notations]

100 Player

101 Data Set Storage Section

102 Data Set Selection Section
103 Address-Data Transmitting Section
104 Random-Number Data Receive Section
105 On the Other Hand, it is Tropism Converter.
106 Data Transmitting Section for Verification
107 Encryption Data Receive Section
108 Decryption Section
907 Mutual Recognition Section
908 Encryption Voice Data Receive Section
909 Voice Playback Section
150 Key Media
151 Extended Address-Data Set Storage Section
152 Address-Data Receive Section
153 Extended Address-Data Extract Section
154 Random-Number Data Generating Section
155 Random-Number Data Transmitting Section
156 On the Other Hand, it is Tropism Converter.
157 Data Receive Section for Verification
158 Verification Section
159 Encryption Data Set Storage Section
160 Encryption Data Extraction Section
161 Encryption Data Transmitting Section
955 Mutual Recognition Section
956 Voice Data Records Department
957 Encryption Section
958 Encryption Voice Data Transmitting Section

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－274791
（P2001－274791A）
(43)公開日　平成13年10月５日(2001.10.5)

(51)Int.Cl.⁷	識別記号	Ｆ Ｉ	テーマコード*(参考)
Ｈ０４Ｌ　9/32		Ｇ０６Ｆ　12/14	３２０Ｂ　５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｇ０９Ｃ　1/00	６６０Ｄ　５Ｊ１０４
Ｇ０９Ｃ　1/00	６６０	Ｈ０４Ｌ　9/00	６７５Ｂ　９Ａ００１
Ｈ０４Ｌ　9/08			６０１Ｃ
			６０１Ｅ

審査請求　未請求　請求項の数13　ＯＬ　（全 17 頁）

(21)出願番号　特願2000－87445(P2000－87445)

(22)出願日　平成12年３月27日(2000.3.27)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　河田　浩嗣
大阪府門真市大字門真1006番地　松下電器産業株式会社内

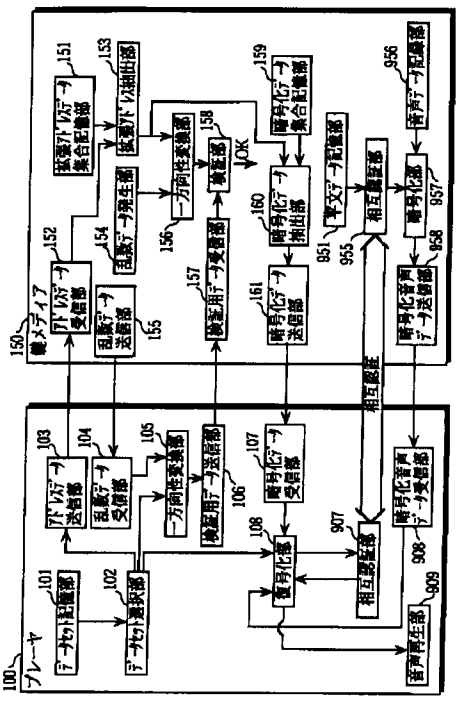
(72)発明者　勝田　昇
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　100090446
弁理士　中島　司朗　（外１名）

最終頁に続く

(54)【発明の名称】　機器認証方法、機器認証システム、受信装置及び送信装置

(57)【要約】
【課題】　不正な受信装置を排除できる機器認証システムを提供する。
【解決手段】　プレーヤ１００は、記憶部１０１が記憶するアドレスデータと拡張アドレスデータと鍵データとのセットの内の１セットを選択（選択部１０２）アドレスデータを送信（送信部１０３）拡張アドレスデータから第１データを生成（変換部１０５）送信（送信部１０６）し、鍵メディア１５０は、これらを受信（受信部１５２、１５７）記憶部１５１に記憶された複数のアドレス付き拡張アドレスデータから拡張アドレスデータを抽出（抽出部１５３）第２データを生成（変換部１５６）第１データと第２データとが同じ値かを検証（検証部１５８）同じ値なら記憶部１５９が記憶する複数の拡張アドレス付き暗号化データから暗号化データを抽出（抽出部１６０）送信（送信部１６１）し、プレーヤ１００は、これを受信（受信部９０８）鍵データで復号化（復号化部１０８）する。



【特許請求の範囲】
【請求項１】　暗号通信の前に、送信装置から受信装置へ通信用データが暗号化された暗号化通信用データを伝送して、受信装置が受信した暗号化通信用データを、自身が保持している複号用鍵データを用いて復号化することにより、送信装置が予め記憶する通信用データを受信装置が共有し、この動作に引き続き、共有した通信用データを用いて暗号通信を行なう暗号通信システムにおける機器認証方法であって、
前記受信装置は、第１アドレスデータと第２アドレスデータと復号用鍵データとからなるデータセットを１セット以上予め記憶しており、
前記送信装置は、第１アドレスデータから第２アドレスデータを特定できる第１アドレス付き第２アドレスデータと、第２アドレスデータから暗号化通信用データを特定できる第２アドレス付き暗号化通信用データとを、それぞれ複数予め記憶しており、
前記受信装置から前記送信装置へ、前記受信装置が予め記憶するデータセットの内の一のデータセットに属する第１アドレスデータを伝送する第１アドレスデータ伝送ステップと、
前記送信装置において、予め記憶している複数の第１アドレス付き第２アドレスデータから、前記受信装置から前記第１アドレスデータ伝送ステップにより伝送された第１アドレスデータにより特定される第２アドレスデータを抽出する第２アドレスデータ抽出ステップと、
前記受信装置における前記一のデータセットに属する第２アドレスデータと、前記送信装置における前記第２アドレスデータ抽出ステップにより抽出された第２アドレスデータとが、同じ値か否かを検証する検証ステップと、
前記検証ステップにより同じ値であると検証された場合に、前記送信装置において、予め記憶している複数の第２アドレス付き暗号化通信用データから、前記第２アドレスデータ抽出ステップにより抽出された第２アドレスデータにより特定される暗号化通信用データを抽出する暗号化通信用データ抽出ステップと、
前記送信装置から前記受信装置へ、前記暗号化通信用データ抽出ステップにより抽出された暗号化通信用データを伝送する暗号化通信用データ伝送ステップと、
前記受信装置において、前記暗号化通信用データ伝送ステップにより伝送された暗号化通信用データを、前記一のデータセットに属する復号用鍵データを用いて復号化して通信用データを生成する復号化ステップとを有することを特徴とする機器認証方法。
【請求項２】　前記検証ステップは、
前記受信装置内、又は、前記送信装置内で乱数データを発生させ、発生させた乱数データを他方に伝送することにより、同じ乱数データを共有する乱数データ共有サブステップと、
前記受信装置において、前記一のデータセットに属する第２アドレスデータと、前記共有した乱数データとに、所定のデータ変換を施して、第１検証用データを生成する第１データ変換サブステップと、
前記受信装置から前記送信装置へ、前記第１検証用データを伝送する第１検証用データ伝送サブステップと、
前記送信装置において、前記第２アドレスデータ抽出ステップにより抽出された第２アドレスデータと、前記共有した乱数データとに、前記第１データ変換サブステップと同じデータ変換を施して、第２検証用データを生成する第２データ変換サブステップと、
前記送信装置において、前記第１検証用データと前記第２検証用データとが同じ値か否かを検証する検証サブステップとを有することを特徴とする請求項１に記載の機器認証方法。
【請求項３】　暗号通信の前に、送信装置から受信装置へ通信用データが暗号化された暗号化通信用データを伝送して、受信装置が受信した暗号化通信用データを、自身が保持している復号用鍵データを用いて復号化することにより、送信装置が予め記憶する通信用データを受信装置が共有し、この動作に引き続き、共有した通信用データを用いて暗号通信を行なう、送信装置と受信装置とからなる機器認証システムであって、
前記受信装置は、
第１アドレスデータと第２アドレスデータと復号用鍵データとからなるデータセットを１セット以上予め記憶するデータセット記憶手段と、
前記送信装置へ、前記データセット記憶手段に記憶されたデータセットの内の一のデータセットに属する第１アドレスデータを送信する第１アドレスデータ送信手段と、
前記一のデータセットに属する第２アドレスデータを元にして、所定のデータ変換を施して、第１検証用データを生成する第１データ変換手段と、
前記送信装置へ、前記第１検証用データを送信する第１検証用データ送信手段と、
前記送信装置から、暗号化通信用データを受信する暗号化通信用データ受信手段と、
前記暗号化通信用データ受信手段により受信された暗号化通信用データを、前記一のデータセットに属する復号用鍵データを用いて復号化して通信用データを生成する復号化手段とを備え、
前記送信装置は、
第１アドレスデータから第２アドレスデータを特定できる第１アドレス付き第２アドレスデータと、第２アドレスデータから暗号化通信用データを特定できる第２アドレス付き暗号化通信用データとを、それぞれ複数予め記憶する集合記憶手段と、
前記受信装置から、第１アドレスデータを受信する第１アドレスデータ受信手段と、

前記集合記憶手段に記憶された複数の第１アドレス付き第２アドレスデータから、前記受信装置から前記第１アドレスデータ受信手段により受信された第１アドレスデータにより特定される第２アドレスデータを抽出する第２アドレスデータ抽出手段と、
前記受信装置から、前記第１検証用データを受信する第１検証用データ受信手段と、
前記第２アドレスデータ抽出手段により抽出された第２アドレスデータを元にして、前記第１データ変換手段と同じデータ変換を施して、第２検証用データを生成する第２データ変換手段と、
前記第１検証用データ受信手段により受信された第１検証用データと前記第２データ変換手段により生成された第２検証用データとが同じ値か否かを検証する検証手段と、
前記検証手段により同じ値であると検証された場合に、予め記憶している複数の第２アドレス付き暗号化通信用データから、前記第２アドレスデータ抽出手段により抽出された第２アドレスデータにより特定される暗号化通信用データを抽出する暗号化通信用データ抽出手段と、
前記受信装置へ、前記暗号化通信用データ抽出手段により抽出された暗号化通信用データを送信する暗号化通信用データ送信手段とを備えることを特徴とする機器認証システム。
【請求項４】　前記受信装置が備える前記第１データ変換手段は、
前記送信装置から、乱数データを受信する乱数データ受信手段を含み、
前記第１データ変換手段は、
前記一のデータセットに属する第２アドレスデータと、前記乱数データ受信手段により受信された乱数データとを元にして、所定のデータ変換を施して、第１検証用データを生成し、
前記送信装置が備える前記第２データ変換手段は、
乱数データを発生させ、発生させた乱数データを前記受信装置に送信する乱数データ発生送信手段を含み、
前記第２データ変換手段は、
前記第２アドレスデータ抽出手段により抽出された第２アドレスデータと、前記乱数データ発生送信手段により発生させた乱数データとを元にして、所定のデータ変換を施して、第２検証用データを生成することを特徴とする請求項３に記載の機器認証システム。
【請求項５】　前記受信装置が備える前記第１データ変換手段は、
乱数データを発生させ、発生させた乱数データを前記送信装置に送信する前記乱数データ発生送信手段を含み、
前記第１データ変換手段は、
前記一のデータセットに属する第２アドレスデータと、前記乱数データ発生送信手段により発生させた乱数データとを元にして、所定のデータ変換を施して、第１検証用データを生成し、
前記送信装置が備える前記第２データ変換手段は、
前記受信装置から、乱数データを受信する乱数データ受信手段を含み、
前記第２データ変換手段は、
前記第２アドレスデータ抽出手段により抽出された第２アドレスデータと、前記乱数データ受信手段により受信された乱数データとを元にして、所定のデータ変換を施して、第２検証用データを生成することを特徴とする請求項３に記載の機器認証システム。
【請求項６】　暗号通信の前に、送信装置から受信装置へ通信用データが暗号化された暗号化通信用データを伝送して、受信装置が受信した暗号化通信用データを、自身が保持している復号用鍵データを用いて復号化することにより、送信装置が予め記憶する通信用データを受信装置が共有し、この動作に引き続き、共有した通信用データを用いて暗号通信を行なう機器認証システムにおける受信装置であって、
第１アドレスデータと第２アドレスデータと復号用鍵データとからなるデータセットを１セット以上予め記憶するデータセット記憶手段と、
前記送信装置へ、前記データセット記憶手段に記憶されたデータセットの内の一のデータセットに属する第１アドレスデータを送信する第１アドレスデータ送信手段と、
前記一のデータセットに属する第２アドレスデータを元にして、所定のデータ変換を施して、検証用データを生成するデータ変換手段と、
前記送信装置へ、前記検証用データを送信する検証用データ送信手段と、
前記送信装置から、暗号化通信用データを受信する暗号化通信用データ受信手段と、
前記暗号化通信用データ受信手段により受信された暗号化通信用データを、前記一のデータセットに属する復号用鍵データを用いて復号化して通信用データを生成する復号化手段とを備えることを特徴とする受信装置。
【請求項７】　前記データ変換手段は、
前記送信装置から、乱数データを受信する乱数データ受信手段を含み、
前記データ変換手段は、
前記一のデータセットに属する第２アドレスデータと、前記乱数データ受信手段により受信された乱数データとを元にして、所定のデータ変換を施して、検証用データを生成することを特徴とする請求項６に記載の受信装置。
【請求項８】　前記データ変換手段は、
乱数データを発生させ、発生させた乱数データを前記送信装置に送信する乱数データ発生送信手段を含み、
前記データ変換手段は、
前記一のデータセットに属する第２アドレスデータと、

前記乱数データ発生送信手段により発生させた乱数データとを元にして、所定のデータ変換を施して、検証用データを生成することを特徴とする請求項６に記載の受信装置。

【請求項９】　暗号通信の前に、送信装置から受信装置へ通信用データが暗号化された暗号化通信用データを伝送して、受信装置が受信した暗号化通信用データを、自身が保持している復号用鍵データを用いて復号化することにより、送信装置が予め記憶する通信用データを受信装置が共有し、この動作に引き続き、共有した通信用データを用いて暗号通信を行なう機器認証システムにおける送信装置であって、

第１アドレスデータから第２アドレスデータを特定できる第１アドレス付き第２アドレスデータと、第２アドレスデータから暗号化通信用データを特定できる第２アドレス付き暗号化通信用データとを、それぞれ複数予め記憶する集合記憶手段と、

前記受信装置から、第１アドレスデータを受信する第１アドレスデータ受信手段と、

前記集合記憶手段に記憶された複数の第１アドレス付き第２アドレスデータから、前記受信装置から前記第１アドレスデータ受信手段により受信された第１アドレスデータにより特定される第２アドレスデータを抽出する第２アドレスデータ抽出手段と、

前記受信装置から、前記第１検証用データを受信する検証用データ受信手段と、

前記第２アドレスデータ抽出手段により抽出された第２アドレスデータを元にして、所定のデータ変換を施して、第２検証用データを生成するデータ変換手段と、

前記検証用データ受信手段により受信された第１検証用データと前記データ変換手段により生成された第２検証用データとが同じ値か否かを検証する検証手段と、

前記検証手段により同じ値であると検証された場合に、予め記憶している複数の第２アドレス付き暗号化通信用データから、前記第２アドレスデータ抽出手段により抽出された第２アドレスデータにより特定される暗号化通信用データを抽出する暗号化通信用データ抽出手段と、

前記受信装置へ、前記暗号化通信用データ抽出手段により抽出された暗号化通信用データを送信する暗号化通信用データ送信手段とを備えることを特徴とする送信装置。

【請求項１０】　前記データ変換手段は、

乱数データを発生させ、発生させた乱数データを前記受信装置に送信する乱数データ発生送信手段を含み、

前記データ変換手段は、

前記第２アドレスデータ抽出手段により抽出された第２アドレスデータと、前記乱数データ発生送信手段により発生させた乱数データとを元にして、所定のデータ変換を施して、第２検証用データを生成することを特徴とする請求項９に記載の送信装置。

【請求項１１】　前記データ変換手段は、

前記受信装置から、乱数データを受信する乱数データ受信手段を含み、

前記データ変換手段は、

前記第２アドレスデータ抽出手段により抽出された第２アドレスデータと、前記乱数データ受信手段により受信された乱数データとを元にして、所定のデータ変換を施して、第２検証用データを生成することを特徴とする請求項９に記載の送信装置。

【請求項１２】　暗号通信の前に、送信装置から受信装置へ通信用データが暗号化された暗号化通信用データを伝送して、受信装置が受信した暗号化通信用データを、自身が保持している復号用鍵データを用いて復号化することにより、送信装置が予め記憶する通信用データを受信装置が共有し、この動作に引き続き、共有した通信用データを用いて暗号通信を行なう機器認証システムにおける受信装置側のプログラムを記録したコンピュータ読み取り可能な記録媒体であって、

前記受信装置は、第１アドレスデータと第２アドレスデータと復号用鍵データとからなるデータセットを１セット以上予め記憶しており、

コンピュータに、

前記送信装置へ、前記受信装置が予め記憶するデータセットの内の一のデータセットに属する第１アドレスデータを送信する第１アドレスデータ送信ステップと、

前記一のデータセットに属する第２アドレスデータを元にして、所定のデータ変換を施して、検証用データを生成するデータ変換ステップと、

前記送信装置へ、前記検証用データを送信する検証用データ送信ステップと、前記送信装置から、暗号化通信用データを受信する暗号化通信用データ受信ステップと、

前記暗号化通信用データ受信ステップにより受信された暗号化通信用データを、前記一のデータセットに属する復号用鍵データを用いて復号化して通信用データを生成する復号化ステップとを実行させることを特徴とする受信装置側のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１３】　暗号通信の前に、送信装置から受信装置へ認証用データが暗号化された暗号化認証用データを伝送して、受信装置が受信した暗号化認証用データを、自身が保持している復号用鍵データを用いて復号化することにより、送信装置が予め記憶する認証用データを受信装置が共有し、この動作に引き続き、共有した認証用データを用いて暗号通信を行なう機器認証システムにおける送信装置側のプログラムを記録したコンピュータ読み取り可能な記録媒体であって、

前記送信装置は、第１アドレスデータから第２アドレスデータを特定できる第１アドレス付き第２アドレスデータと、第２アドレスデータから暗号化通信用データを特定できる第２アドレス付き暗号化通信用データとを、そ

れぞれ複数予め記憶しており、
コンピュータに、
前記受信装置から、第１アドレスデータを受信する第１アドレスデータ受信ステップと、
前記受信装置が予め記憶している複数の第１アドレス付き第２アドレスデータから、前記受信装置から前記第１アドレスデータ受信ステップにより受信された第１アドレスデータにより特定される第２アドレスデータを抽出する第２アドレスデータ抽出ステップと、
前記受信装置から、前記第１検証用データを受信する検証用データ受信ステップと、
前記第２アドレスデータ抽出ステップにより抽出された第２アドレスデータを元にして、所定のデータ変換を施して、第２検証用データを生成するデータ変換ステップと、
前記検証用データ受信ステップにより受信された第１検証用データと前記データ変換ステップにより生成された第２検証用データとが同じ値か否かを検証する検証ステップと、
前記検証ステップにより同じ値であると検証された場合に、予め記憶している複数の第２アドレス付き暗号化通信用データから、前記第２アドレスデータ抽出ステップにより抽出された第２アドレスデータにより特定される暗号化通信用データを抽出する暗号化通信用データ抽出ステップと、
前記受信装置へ、前記暗号化通信用データ抽出ステップにより抽出された暗号化通信用データを送信する暗号化通信用データ送信ステップと実行させることを特徴とする送信装置側のプログラムを記録したコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は暗号化通信を行う装置に関し、特に、通信を開始する前に通信相手の装置が正しいか否かを確かめる為の機器認証技術に関する。
【０００２】
【従来の技術】一般に暗号化通信においては、送信側の装置が暗号化鍵を用いて平文データを暗号化して通信路を介して送信し、これを受信側の装置が受信して復号鍵を用いて復号化することによって平文データを取得する。この様に、通信路には暗号化されたデータだけが送出されることになるので、通信路上のデータが第三者によって傍受されたとしても平文データを知られることがなく安全である。ここで、暗号化されたデータを送受信する通信路をＳＥＣＵＲＥ　ＡＵＴＨＥＮＴＩＣＡＴＥＤ　ＣＨＡＮＮＥＬと呼ぶ。
【０００３】また、受信側の装置が適切な復号鍵を持った正しい受信機であることを、送信側の装置が、ＳＥＣＵＲＥ　ＡＵＴＨＥＮＴＩＣＡＴＥＤ　ＣＨＡＮＮＥＬを開くに先駆けて確認する機器認証処理が広く実施されている。一方、音楽等のデジタル音声データは、コピーされるとオリジナルとまったく同じものができてしまうため、著作権保護の観点から安易にコピーされないようにしたいという要求が強い。そこで記録しているデジタル音声データを必ず暗号化して出力するメモリカードが登場した。このメモリカードは再生用のオーディオ機器と相互認証を行ない、正しい受信機であると認証したオーディオ機器へ、相互認証の過程で生成した共通鍵データを用いて暗号化したデジタル音声データを送信する。
【０００４】図３は、従来の暗号化通信における機器認証処理の概略を説明する為の暗号化通信システムを示す図である。図３に示す暗号化通信システムは、プレーヤ９００及び鍵メディア９５０からなる。ここで、プレーヤとは暗号化されたデジタル音声データを受信して音声を再生することができるオーディオ機器等であり、鍵メディアとは記録しているデジタル音声データを暗号化して送信する機能を備えたメモリスティック等であるものとする。
【０００５】プレーヤ９００は、認証要求部９０１、暗号化データ集合受信部９０２、データセット記憶部９０３、データセット選択部９０４、暗号化データ抽出部９０５、復号化部９０６、相互認証部９０７、暗号化音声データ受信部９０８、及び、音声再生部９０９を備える。認証要求部９０１は、鍵メディア９５０に機器認証を要求する。
【０００６】暗号化データ集合受信部９０２は、認証要求部９０１による機器認証の要求の後に、鍵メディア９５０からアドレス付き暗号化データ集合を受信する。ここでアドレス付き暗号化データ集合とは、鍵メディア９５０に予め記憶されている共通の平文データを共通の暗号化手段によりいろいろな鍵データを用いて暗号化して得られた暗号化データの集合であり、それぞれの暗号化データにはアドレスが付いていて、このアドレスのデータから暗号化データを特定できる。ここでは１個の暗号化データは８バイトであり、アドレス付き暗号化データ集合は、１６行×５１２列（８Ｋ）個のアドレス付き暗号化データの集合とする。
【０００７】データセット記憶部９０３は、アドレスデータと鍵データとからなるデータセットを１セット以上予め記憶している。ここであるデータセット中のアドレスデータが示すアドレスは、暗号化データ集合受信部９０２で受信するアドレス付き暗号化データ集合の中の何れかのアドレスと一致する様になっており、このアドレスが付加された暗号化データは、このデータセット中の鍵データを用いて暗号化されたものとなっている。ここでは１６個のデータセットを予め記憶する。
【０００８】データセット選択部９０４は、データセット記憶部９０３に予め記憶された１セット以上のデータセットの中から１セットを任意に選択する。暗号化データ抽出部９０５は、暗号化データ集合受信部９０２によ

り受信されたアドレス付き暗号化データ集合から、データセット選択部９０４により選択されたデータセット中のアドレスデータにより特定される暗号化データを抽出する。

【０００９】復号化部９０６は、暗号化データ抽出部９０５により抽出された暗号化データをデータセット選択部９０４により選択されたデータセット中の鍵データを用いて復号化して平文データを生成し、さらに、相互認証部９０７が生成する共有鍵を用いて、鍵メディア９５０から受信する暗号化音声データを復号化して音声データを生成する。

【００１０】相互認証部９０７は、プレーヤと鍵メディアとの間で相互に機器認証する相互認証処理を行なうものであり、復号化部９０６により復号化された平文データと鍵メディア９５０から受信する第１乱数データとを用いて、予め定めた所定の一方向性変換を行なって、鍵メディア９５０に対して自身が正しい受信機であることを示すプレーヤ認証用データを生成して送信する。また、自ら第１乱数データを発生させて鍵メディア９５０に送信し、鍵メディア９５０が正しい送信機であることを示す鍵メディア認証用データを受信して、前記平文データと自ら発生させた第１乱数データとを用いて前記一方向性変換を行なって生成した鍵メディア認証用データと一致する場合に、正しい送信機であると認証する。さらに、鍵メディア９５０から受信する暗号化音声データを復号化する為に用いる共有鍵を生成する。

【００１１】ここで共有鍵は、受信した第１乱数データと自ら発生させた第２乱数データとを排他的論理和した加算乱数データと前記平文データとを用いて前記一方向性変換を行なって生成する。また暗号化音声データは、鍵メディア９５０が当該プレーヤ９００を正しい受信機であると認証した場合にのみ送信される。

【００１２】暗号化音声データ受信部９０８は、鍵メディア９５０から暗号化音声データを受信する。音声再生部９０９は、復号化部９０６により復号化されて生成された音声データを用いて音声を再生する。鍵メディア９５０は、平文データ記憶部９５１、認証要求受付部９５２、暗号化データ集合記憶部９５３、暗号化データ集合送信部９５４、相互認証部９５５、音声データ記録部９５６、暗号化部９５７、及び、暗号化音声データ送信部９５８を備える。

【００１３】平文データ記憶部９５１は、所定の平文データを予め１つ記憶する。ここでは、７バイトの平文データを１つ予め記憶する。認証要求受付部９５２は、プレーヤ９００より認証要求を受付ける。暗号化データ集合記憶部９５３は、アドレス付き暗号化データ集合を予め記憶する。ここではアドレス付き暗号化データ集合は１６行×５１２列（８Ｋ）個のアドレス付き暗号化データの集合とし、１個の暗号化データは８バイトとする。

【００１４】暗号化データ集合送信部９５４は、認証要求受付部９５１により認証要求が受付けられた場合に、暗号化データ集合記憶部９５２に記憶された暗号化データ集合を返送する。相互認証部９５５は、相互認証部９０７と共に相互認証処理を行なうものであり、自ら第２乱数データを発生させてプレーヤ９００に送信し、プレーヤ認証用データを受信して、平文データ記憶部９５１に記憶された平文データと自ら発生させた第２乱数データとを用いて、相互認証部９０７と同じ一方向性変換を行なって生成したプレーヤ認証用データと一致する場合に、正しい受信機であると認証する。また、前記平文データとプレーヤ９００から受信する第２乱数データとを用いて、前記一方向性変換を行なって、鍵メディア認証用データを生成して送信する。さらに、音声データ記録部９５６に記録された音声データをプレーヤ９００へ送信する暗号化音声データに暗号化する為に用いる共有鍵を生成する。

【００１５】ここで共有鍵は、自ら発生させた第１乱数データと受信した第２乱数データとを排他的論理和した加算乱数データと前記平文データとを用いて前記一方向性変換を行なって生成する。音声データ記録部９５６は音声データを記録する。暗号化部９５７は、相互認証部９５５によりプレーヤ９００が正しい受信機であると認証された場合に、音声データ記録部９５６に記録された音声データを、相互認証部９５５により生成された共有鍵を用いて暗号化して暗号化音声データを生成する。

【００１６】暗号化音声データ送信部９５８は、暗号化部９５７により生成された暗号化音声データをプレーヤ９００に送信する。ここで、従来の暗号化通信における平文データの共有、相互認証処理、共有鍵の生成、暗号化音声データの送受信及び音声の再生の動作を説明する。

（１）プレーヤ９００の認証要求部９０１が、鍵メディア９５０に機器認証を要求する。

（２）鍵メディア９５０の認証要求受付部９５１が、機器認証の要求を受付ける。

（３）鍵メディア９５０が機器認証の要求を受付けると、鍵メディア９５０の暗号化データ集合送信部９５３が、暗号化データ集合記憶部９５２に記憶された暗号化データ集合を返送する。

（４）プレーヤ９００の暗号化データ集合受信部９０２が、返送されたアドレス付き暗号化データ集合を受信する。

（５）プレーヤ９００のデータセット選択部９０４が、データセット記憶部９０３に予め記憶されたデータセットの中から１セットを任意に選択する。

（６）プレーヤ９００の暗号化データ抽出部９０５が、暗号化データ集合受信部９０２により受信されたアドレス付き暗号化データ集合から、データセット選択部９０４により選択されたデータセット中のアドレスデータにより特定される暗号化データを抽出する。

（７）プレーヤ９００の復号化部９０６が、暗号化データ抽出部９０５により抽出された暗号化データを当該データセット中の鍵データを用いて復号化して平文データを生成する。
（８）鍵メディア９５０の相互認証部９５５が第１乱数データを発生させてプレーヤ９００へ送信する。
（９）プレーヤ９００の相互認証部９０７が、鍵メディア９５０から第１乱数データを受信し、復号化部９０６により復号化された平文データと受信した第１乱数データとを用いて、予め定めた所定の一方向性変換を行なって、プレーヤ認証用データを生成して鍵メディア９５０へ送信し、第２乱数データを発生させて鍵メディア９５０へ送信する。
（１０）鍵メディア９５０の相互認証部９５５が、プレーヤ認証用データを受信し、前記平文データと自ら発生させた第１乱数データとを用いて前記一方向性変換を行なってプレーヤ認証用データを生成し、両者が一致する場合にプレーヤ９００が正しい受信機であると認証する。一致しない場合は処理を止める。
（１１）プレーヤ９００が正しい受信機であると認証されたなら、鍵メディア９５０の相互認証部９５５がプレーヤ９００から第２乱数データを受信し、平文データ記憶部９５１に記憶された平文データと受信した第２乱数データとを用いて、前記一方向性変換を行なって、鍵メディア認証用データを生成してプレーヤ９００へ送信し、自ら発生させた第１乱数データと受信した第２乱数データとを排他的論理和した加算乱数データと前記平文データとを用いて前記一方向性変換を行なって共有鍵を生成する。
（１２）プレーヤ９００の相互認証部９０７が、鍵メディア認証用データを受信し、前記平文データと自ら発生させた第２乱数データとを用いて前記一方向性変換を行なって鍵メディア認証用データを生成し、両者が一致する場合に鍵メディア９５０が正しい送信機であると認証する。一致しない場合は処理を止める。
（１３）鍵メディア９５０が正しい送信機であると認証されたなら、プレーヤ９００の相互認証部９０７が、受信した第１乱数データと自ら発生させた第２乱数データとを排他的論理和した加算乱数データと前記平文データとを用いて前記一方向性変換を行なって共有鍵を生成する。
（１４）鍵メディア９５０の暗号化部９５７が、音声データ記録部９５６に記録された音声データを、相互認証部９５５により生成された共有鍵を用いて暗号化して暗号化音声データを生成する。
（１５）鍵メディア９５０の暗号化音声データ送信部９５８が、暗号化部９５７により生成された暗号化音声データをプレーヤ９００に送信する。
（１６）プレーヤ９００の暗号化音声データ受信部９０８が、鍵メディア９５０から暗号化音声データを受信する。
（１７）プレーヤ９００の復号化部９０６が、相互認証部９０７により生成された共有鍵を用いて、鍵メディア９５０から受信した暗号化音声データを復号化して音声データを生成する。
（１８）プレーヤ９００の音声再生部９０９が、復号化部９０６により復号化されて生成された音声データを用いて音声を再生する。
【００１７】以上のように、従来の暗号化通信システムは、プレーヤが適切な鍵データを少なくとも１個以上保持していることによって鍵メディアがプレーヤを正しい受信機であると認識して、鍵メディアが記録しているデータの出力を許可するという仕組みを備えているのである。さらに上記のような従来の暗号化通信システムにおいて、鍵メディアは、何らかの理由で不正であるとみなされたプレーヤを排除する機能を有している。正確には、不正であるとみなされた以後に製造又は発売される鍵メディアを、不正であるとみなされたプレーヤにおいて使えなくすることができるのである。
【００１８】鍵メディア９５０の暗号化データ集合記憶部９５３には、発売当初において全て有効なアドレス付き暗号化データが例えば８Ｋ個記憶されているものとする。プレーヤ９００のデータセット記憶部９０３には例えば１６個のデータセットが記憶されており、それぞれ鍵メディア９５０の暗号化データ集合記憶部９５３の８Ｋ個のうちの何れかに対応しており、プレーヤのメーカーや機種によって異なる組み合わせとなっている。
【００１９】ここで何らかの理由で、あるプレーヤが不正であるとみなされると、不正であるとみなされたプレーヤのデータセット記憶部９０３に記憶された１６個のデータセットに対応する暗号化データを、それ以後に製造又は発売される鍵メディア９５０の暗号化データ集合記憶部９５３に記憶された暗号化データ集合において全て無効なデータに置き変えるのである。
【００２０】こうすることによって、不正であるとみなされたプレーヤのデータセット記憶部に記憶されたデータセットが全て無効になるので、不正であるとみなされたプレーヤはその鍵メディアからデータを読み出せなくなる。なお、他のプレーヤは１６個のデータセットが１つでも有効であれば鍵メディアからデータを読み出すことができるので、他種類のプレーヤに対応できる。
【００２１】
【発明の解決しようとする課題】ここであるプレーヤが、不正であるとみなされる前に正当に取得した平文データを蓄え、不正であるとみなされた以後において、自分が保持していない適当な鍵データのデータアドレスを鍵メディアに送信して暗号化データを得て、この暗号化データを復号化せずに予め蓄えておいた平文データを用いて以後の処理を進めることで、このプレーヤは正しい受信機になりすますことができる。

【００２２】プレーヤがこのような処理を行うと、鍵メディアはプレーヤから送信されたデータアドレスに対応する鍵データをそのプレーヤが保持していないにもかかわらずそのプレーヤを正しい受信機であると錯覚してしまうので、プレーヤが適切な鍵データを保持していることによって鍵メディアがプレーヤを正しい受信機であると認識して、鍵メディアが記録しているデータの出力を許可するという仕組みが適正に機能しなくなる。

【００２３】そこで本発明は、受信装置が不正であるとみなされる前に平文データを蓄えようとも、不正であるとみなされた受信装置を排除することができる機器認証システム、送信装置、受信装置、それらの方法、及び、それらのプログラムを記録した記録媒体を提供することを目的とする。

【００２４】

【課題を解決するための手段】上記目的を達成するために、本発明に係る機器認証方法は、暗号通信の前に送信装置から受信装置へ通信用データが暗号化された暗号化通信用データを伝送して、受信装置が受信した暗号化通信用データを自身が保持している複号用鍵データを用いて復号化することにより送信装置が予め記憶する通信用データを受信装置が共有し、この動作に引き続き共有した通信用データを用いて暗号通信を行なう暗号通信システムにおける機器認証方法であって、前記受信装置は第１アドレスデータと第２アドレスデータと復号用鍵データとからなるデータセットを１セット以上予め記憶しており、前記送信装置は第１アドレスデータから第２アドレスデータを特定できる第１アドレス付き第２アドレスデータと、第２アドレスデータから暗号化通信用データを特定できる第２アドレス付き暗号化通信用データとをそれぞれ複数予め記憶しており、前記受信装置から前記送信装置へ前記受信装置が予め記憶するデータセットの内の一のデータセットに属する第１アドレスデータを伝送する第１アドレスデータ伝送ステップと、前記送信装置において予め記憶している複数の第１アドレス付き第２アドレスデータから前記受信装置から前記第１アドレスデータ伝送ステップにより伝送された第１アドレスデータにより特定される第２アドレスデータを抽出する第２アドレスデータ抽出ステップと、前記受信装置における前記一のデータセットに属する第２アドレスデータと前記送信装置における前記第２アドレスデータ抽出ステップにより抽出された第２アドレスデータとが同じ値か否かを検証する検証ステップと、前記検証ステップにより同じ値であると検証された場合に前記送信装置において予め記憶している複数の第２アドレス付き暗号化通信用データから前記第２アドレスデータ抽出ステップにより抽出された第２アドレスデータにより特定される暗号化通信用データを抽出する暗号化通信用データ抽出ステップと、前記送信装置から前記受信装置へ前記暗号化通信用データ抽出ステップにより抽出された暗号化通信用データを伝送する暗号化通信用データ伝送ステップと、前記受信装置において前記暗号化通信用データ伝送ステップにより伝送された暗号化通信用データを前記一のデータセットに属する復号用鍵データを用いて復号化して通信用データを生成する復号化ステップとを有することを特徴とする。

【００２５】上記目的を達成するために、本発明に係る機器認証システムは、暗号通信の前に送信装置から受信装置へ通信用データが暗号化された暗号化通信用データを伝送して、受信装置が受信した暗号化通信用データを自身が保持している復号用鍵データを用いて復号化することにより送信装置が予め記憶する通信用データを受信装置が共有し、この動作に引き続き共有した通信用データを用いて暗号通信を行なう送信装置と受信装置とからなる機器認証システムであって、前記受信装置は、第１アドレスデータと第２アドレスデータと復号用鍵データとからなるデータセットを１セット以上予め記憶するデータセット記憶手段と、前記送信装置へ前記データセット記憶手段に記憶されたデータセットの内の一のデータセットに属する第１アドレスデータを送信する第１アドレスデータ送信手段と、前記一のデータセットに属する第２アドレスデータを元にして所定のデータ変換を施して、第１検証用データを生成する第１データ変換手段と、前記送信装置へ前記第１検証用データを送信する第１検証用データ送信手段と、前記送信装置から暗号化通信用データを受信する暗号化通信用データ受信手段と、前記暗号化通信用データ受信手段により受信された暗号化通信用データを前記一のデータセットに属する復号用鍵データを用いて復号化して通信用データを生成する復号化手段とを備え、前記送信装置は、第１アドレスデータから第２アドレスデータを特定できる第１アドレス付き第２アドレスデータと第２アドレスデータから暗号化通信用データを特定できる第２アドレス付き暗号化通信用データとをそれぞれ複数予め記憶する集合記憶手段と、前記受信装置から第１アドレスデータを受信する第１アドレスデータ受信手段と、前記集合記憶手段に記憶された複数の第１アドレス付き第２アドレスデータから前記受信装置から前記第１アドレスデータ受信手段により受信された第１アドレスデータにより特定される第２アドレスデータを抽出する第２アドレスデータ抽出手段と、前記受信装置から前記第１検証用データを受信する第１検証用データ受信手段と、前記第２アドレスデータ抽出手段により抽出された第２アドレスデータを元にして前記第１データ変換手段と同じデータ変換を施して第２検証用データを生成する第２データ変換手段と、前記第１検証用データ受信手段により受信された第１検証用データと前記第２データ変換手段により生成された第２検証用データとが同じ値か否かを検証する検証手段と、前記検証手段により同じ値であると検証された場合に予め記憶している複数の第２アドレス付き暗号化通信用デ

ータから前記第２アドレスデータ抽出手段により抽出された第２アドレスデータにより特定される暗号化通信用データを抽出する暗号化通信用データ抽出手段と、前記受信装置へ前記暗号化通信用データ抽出手段により抽出された暗号化通信用データを送信する暗号化通信用データ送信手段とを備えることを特徴とする。

【００２６】

【発明の実施の形態】＜概要＞本発明は、送信装置がアドレス付き拡張アドレスデータ集合と拡張アドレス付き暗号化データ集合とを予め記憶し、受信装置（プレーヤ）がアドレスデータと拡張アドレスデータと鍵データとからなるデータセットを１セット以上予め記憶し、暗号化データのアドレスを間接参照とし、暗号通信を始める前に、送信装置（鍵メディア）が、拡張アドレスデータを用いて受信装置が正当であることを検証した後、従来の様に暗号化データ集合全部を送受信せずに、この拡張アドレスデータと対応する暗号化データのみを受信装置へ送信する暗号化通信システムであり、暗号化データは受信装置で復号化されて平文データとなることで平文データが共有され、この平文データを用いて暗号通信が行われる。

【００２７】＜構成＞図１は、本実施の形態に係る暗号化通信システムの構成を示す図である。図１に示す暗号化通信システムは、プレーヤ１００及び鍵メディア１５０からなる。プレーヤ１００は、暗号化されたデジタル音声データを受信して音声を再生することができるオーディオ機器等であって暗号通信に用いられる平文データの元になる暗号化データを送信される前に鍵メディア１５０に正当な受信機であるかを検証されるものであり、データセット記憶部１０１、データセット選択部１０２、アドレスデータ送信部１０３、乱数データ受信部１０４、一方向性変換部１０５、検証用データ送信部１０６、暗号化データ受信部１０７、復号化部１０８、相互認証部９０７、暗号化音声データ受信部９０８、及び、音声再生部９０９を備える。

【００２８】鍵メディア１５０は、記録しているデジタル音声データを暗号化して送信する機能を備えたメモリスティック等であって暗号化データを送信する前にプレーヤ１００が正当な受信機であるかを検証するものであり、平文データ記憶部９５１、拡張アドレスデータ集合記憶部１５１、アドレスデータ受信部１５２、拡張アドレスデータ抽出部１５３、乱数データ発生部１５４、乱数データ送信部１５５、一方向性変換部１５６、検証用データ受信部１５７、検証部１５８、暗号化データ集合記憶部１５９、暗号化データ抽出部１６０、暗号化データ送信部１６１、相互認証部９５５、音声データ記録部９５６、暗号化部９５７、及び、暗号化音声データ送信部９５８を備える。ここで、従来の暗号化通信システムにおける構成要素と同じ番号で示した構成要素は、同様の機能を有するものとしその説明を省略する。

【００２９】データセット記憶部１０１は、アドレスデータと拡張アドレスデータと鍵データとからなるデータセットを１セット以上予め記憶している。ここでは１６個のデータセットを予め記憶する。データセット選択部１０２は、データセット記憶部１０１に予め記憶された１セット以上のデータセットの中から１セットのデータセットを任意に選択する。

【００３０】アドレスデータ送信部１０３は、データセット選択部１０２により選択されたデータセット中のアドレスデータを鍵メディア１５０へ送信する。乱数データ受信部１０４は、鍵メディア１５０から乱数データを受信する。一方向性変換部１０５は、データセット選択部１０２により選択されたデータセット中の拡張アドレスデータと、乱数データ受信部１０４により受信された乱数データとを用いて一方向性変換を行なって検証用データを生成する。

【００３１】検証用データ送信部１０６は、一方向性変換部１０５が生成した検証用データを鍵メディア１５０へ送信する。暗号化データ受信部１０７は、暗号化データを鍵メディア１５０から受信する。ここでは８バイトの暗号化データ１個を受信する。復号化部１０８は、暗号化データ受信部１０７により受信された暗号化データをデータセット選択部１０２により選択されたデータセット中の鍵データを用いて復号化して平文データを生成し、さらに、相互認証部９０７が生成する共有鍵を用いて、鍵メディア１５０から受信する暗号化音声データを復号化して音声データを生成する。

【００３２】拡張アドレスデータ集合記憶部１５１は、アドレス付き拡張アドレスデータ集合を記憶する。ここでアドレス付き拡張アドレスデータ集合とは、暗号化データ集合記憶部１５９に記憶された拡張アドレス付き暗号化データ集合中の拡張アドレスを示すデータの集合であり、それぞれの拡張アドレスデータにはアドレスが付いていて、このアドレスのデータから拡張アドレスデータを特定できる。ここではアドレス付き拡張アドレスデータ集合は１６行×５１２列（８Ｋ）個のアドレス付き拡張アドレスデータの集合とする。

【００３３】アドレスデータ受信部１５２は、アドレスデータをプレーヤ１００から受信する。拡張アドレスデータ抽出部１５３は、拡張アドレスデータ集合記憶部１５１に記憶されたアドレス付き拡張アドレスデータ集合から、アドレスデータ受信部１５２により受信されたアドレスデータが示すアドレスが付加された拡張アドレスデータを抽出する。

【００３４】乱数データ発生部１５４は、乱数データを発生させる。乱数データ送信部１５５は、乱数データ発生部１５４が発生させた乱数データを、プレーヤ１００へ送信する。一方向性変換部１５６は、拡張アドレスデータ抽出部１５３により抽出された拡張アドレスデータと、乱数データ発生部１５４により発生された乱数デー

タとを用いて一方向性変換を行なって検証用データを生成する。

【００３５】検証用データ受信部１５７は、検証用データをプレーヤ１００から受信する。検証部１５８は、一方向性変換部１５６により生成された検証用データと、検証用データ受信部１５７により受信された検証用データとが同じ値であるか否かを検証する。暗号化データ集合記憶部１５９は、拡張アドレス付き暗号化データ集合を記憶する。ここで拡張アドレス付き暗号化データ集合とは、鍵メディア１５０の平文データ記憶部９５１に予め記憶されている共通の平文データを共通の暗号化手段によりいろいろな鍵データを用いて暗号化して得られた暗号化データの集合であり、それぞれの暗号化データには拡張アドレスが付いていて、この拡張アドレスのデータから暗号化データを特定できる。ここでは１個の暗号化データは８バイトであり、拡張アドレス付き暗号化データ集合は、１６行×５１２列（８Ｋ）個の拡張アドレス付き暗号化データの集合とする。

【００３６】暗号化データ抽出部１６０は、検証用データが同じ値である場合に暗号化データ集合記憶部１５９に記憶された拡張アドレス付き暗号化データ集合から、拡張アドレスデータ抽出部１５３により抽出された拡張アドレスデータにより特定される暗号化データを抽出する。暗号化データ送信部１６１は、暗号化データ抽出部１６０により抽出された暗号化データをプレーヤ１００へ送信する。ここでは８バイトの暗号化データ１個を送信する。

【００３７】＜動作＞ここで、本実施の形態の暗号化通信における、平文データの共有、相互認証処理、共有鍵の生成、暗号化音声データの送受信及び音声の再生の動作を説明する。図２は、本実施の形態の暗号化通信システムの動作の一例を示す図である。

（１）プレーヤ１００のデータセット選択部１０２が、データセット記憶部１０１に予め記憶された１セット以上のデータセットの中から１セットのデータセットを任意に選択する（ステップＳ１）。

（２）プレーヤ１００のアドレスデータ送信部１０３が、データセット選択部１０２により選択されたデータセット中のアドレスデータを鍵メディア１５０へ送信する（ステップＳ２）。

（３）鍵メディア１５０のアドレスデータ受信部１５２が、アドレスデータをプレーヤ１００から受信する（ステップＳ３）。

（４）鍵メディア１５０の拡張アドレスデータ抽出部１５３が、拡張アドレスデータ集合記憶部１５１に記憶されたアドレス付き拡張アドレスデータ集合から、アドレスデータ受信部１５２により受信されたアドレスデータにより特定される拡張アドレスデータを抽出する（ステップＳ４）。

（５）鍵メディア１５０の乱数データ発生部１５４が、乱数データを発生させる（ステップＳ５）。

（６）鍵メディア１５０の乱数データ送信部１５５が、乱数データ発生部１５４が発生させた乱数データを、プレーヤ１００へ送信する（ステップＳ６）。

（７）プレーヤ１００の乱数データ受信部１０４が、鍵メディア１５０から乱数データを受信する（ステップＳ７）。

（８）プレーヤ１００の一方向性変換部１０５が、データセット選択部１０２により選択されたデータセット中の拡張アドレスデータと、乱数データ受信部１０４により受信された乱数データとを用いて一方向性変換を行なって検証用データを生成する（ステップＳ８）。

（９）プレーヤ１００の検証用データ送信部１０６が、一方向性変換部１０５が生成した検証用データを鍵メディア１５０へ送信する（ステップＳ９）。

（１０）鍵メディア１５０の一方向性変換部１５６が、拡張アドレスデータ抽出部１５３により抽出された拡張アドレスデータと、乱数データ発生部１５４により発生された乱数データとを用いて一方向性変換を行なって検証用データを生成する（ステップＳ１０）。

（１１）鍵メディア１５０の検証部１５８は、一方向性変換部１５６により生成された検証用データと、検証用データ受信部１５７により受信された検証用データとが同じ値であるか否かを検証する（ステップＳ１１）。同じ値でない場合は以後の処理を止める。

（１２）検証用データが同じ値である場合は、鍵メディア１５０の暗号化データ抽出部１６０が、暗号化データ集合記憶部１５９に記憶された拡張アドレス付き暗号化データ集合から、拡張アドレスデータ抽出部１５３により抽出された拡張アドレスデータにより特定される暗号化データを抽出する（ステップＳ１２）。

（１３）鍵メディア１５０の暗号化データ送信部１６１が、暗号化データ抽出部１６０により抽出された暗号化データをプレーヤ１００へ送信する（ステップＳ１３）。

（１４）プレーヤ１００の暗号化データ受信部１０７が、暗号化データを鍵メディア１５０から受信する（ステップＳ１４）。

（１５）プレーヤ１００の復号化部１０８が、暗号化データ受信部１０７により受信された暗号化データをデータセット選択部１０２により選択されたデータセット中の鍵データを用いて復号化して平文データを生成する（ステップＳ１５）。

【００３８】ここまでで平文データの共有までは完了した。以下に説明する相互認証処理、共有鍵の生成、暗号化音声データの送受信及び音声の再生の動作（ステップＳ１６）は、従来の技術で説明したものと同様である。

（１６）鍵メディア１５０の相互認証部９５５が第１乱数データを発生させてプレーヤ９００へ送信する。

（１７）プレーヤ１００の相互認証部９０７が、鍵メデ

ィア１５０から第１乱数データを受信し、復号化部１０８により復号化された平文データと受信した第１乱数データとを用いて、予め定めた所定の一方向性変換を行なって、プレーヤ認証用データを生成して鍵メディア１５０へ送信し、第２乱数データを発生させて鍵メディア１５０へ送信する。

（１８）鍵メディア１５０の相互認証部９５５が、プレーヤ認証用データを受信し、前記平文データと自ら発生させた第１乱数データとを用いて前記一方向性変換を行なってプレーヤ認証用データを生成し、両者が一致する場合にプレーヤ１００が正しい受信機であると認証する。一致しない場合は処理を止める。

（１９）プレーヤ１００が正しい受信機であると認証されたなら、鍵メディア１５０の相互認証部９５５がプレーヤ１００から第２乱数データを受信し、平文データ記憶部９５１に記憶された平文データと受信した第２乱数データとを用いて、前記一方向性変換を行なって、鍵メディア認証用データを生成してプレーヤ１００へ送信し、自ら発生させた第１乱数データと受信した第２乱数データとを排他的論理和した加算乱数データと前記平文データとを用いて前記一方向性変換を行なって共有鍵を生成する。

（２０）プレーヤ１００の相互認証部９０７が、鍵メディア認証用データを受信し、前記平文データと自ら発生させた第２乱数データとを用いて前記一方向性変換を行なって鍵メディア認証用データを生成し、両者が一致する場合に鍵メディア９５０が正しい送信機であると認証する。一致しない場合は処理を止める。

（２１）鍵メディア１５０が正しい送信機であると認証されたなら、プレーヤ１００の相互認証部９０７が、受信した第１乱数データと自ら発生させた第２乱数データとを排他的論理和した加算乱数データと前記平文データとを用いて前記一方向性変換を行なって共有鍵を生成する。

（２２）鍵メディア１５０の暗号化部９５７が、音声データ記録部９５６に記録された音声データを、相互認証部９５５により生成された共有鍵を用いて暗号化して暗号化音声データを生成する。

（２３）鍵メディア１５０の暗号化音声データ送信部９５８が、暗号化部９５７により生成された暗号化音声データをプレーヤ１００に送信する。

（２４）プレーヤ１００の暗号化音声データ受信部９０８が、鍵メディア１５０から暗号化音声データを受信する。

（２５）プレーヤ１００の復号化部１０８が、相互認証部９０７により生成された共有鍵を用いて、鍵メディア１５０から受信した暗号化音声データを復号化して音声データを生成する。

（２６）プレーヤ１００の音声再生部９０９が、復号化部１０８により復号化されて生成された音声データを用いて音声を再生する。

【００３９】以上のように、本実施の形態の暗号化通信システムによれば、プレーヤ１００は、鍵メディア１５０に送信したアドレスデータに対応する拡張アドレスデータを保持している場合にのみ、暗号化データを得ることができる。従って、プレーヤ１００は自分の保持していない適当なアドレスデータを鍵メディア１５０に送信しても暗号化データを得ることはできず、正しい受信機になりすますことができなくなる。

【００４０】なお、本実施の形態では、鍵メディア１５０が乱数データ発生部と乱数データ発生部とを備えたが、これらをプレーヤ１００が備えてもよい。要は、プレーヤ１００内、又は、鍵メディア１５０内で乱数データを発生させ、発生させた乱数データを他方に伝送することにより、同じ乱数データを共有できればよい。また、一方向性変換部１０５と一方向性変換部１５６とが行なう一方向性変換は、必ずしも乱数データを用いなくてもよい。また、ここで行なうデータ変換はかならずしも一方向性変換でなくてもよく、この２つの変換部が同じデータ変換を行なうものであれば何であってもよい。但し、本実施の形態のように乱数データを用いて一方向性変換を行なうと、データ変換された拡張アドレスデータが通信路上で第三者によって傍受されたとしても拡張アドレスデータを知られる危険が極めて低く安全である。

【００４１】また、乱数データ発生部や一方向性変換部は、元々、従来の相互認証部９０７や相互認証部９５５に含まれており、これらと共用することができるので、ハードウェア及びソフトウェアの追加が少なくて済む。また、本実施の形態では、暗号化データ集合記憶部１５９が拡張アドレス付き暗号化データ集合を記憶したが、アドレス付き暗号化データ集合を記憶してもよい。この様な場合には、暗号化データ抽出部１６０が暗号化データ集合記憶部１５９に記憶されたアドレス付き暗号化データ集合から、アドレスデータ受信部１５２により受信されたアドレスデータにより特定される暗号化データを抽出する。

【００４２】また、本実施の形態は、音声を再生することができるオーディオ機器等とメモリスティック等を例にして説明したが、暗号化通信を行なう如何なる装置に適応してもよい。例えば、インターネット等の通信回線を介して、何らかのデータをパソコン間で送受信するものであってもよい。また、コンピュータに本実施の形態のような動作を実行させることができるプログラムが、コンピュータ読み取り可能な記録媒体に記録され、この記録媒体が流通し、取り引きの対象となりうる。

【００４３】ここでコンピュータ読み取り可能な記録媒体とは、例えば、フロッピー（登録商標）ディスク、ＣＤ、ＭＯ、ＤＶＤ、メモリーカード等の着脱可能な記録媒体、及び、ハードディスク、半導体メモリ等の固定記

録媒体等であり、特に限定されるものではない。

【００４４】

【発明の効果】本発明に係る機器認証方法は、暗号通信の前に送信装置から受信装置へ通信用データが暗号化された暗号化通信用データを伝送して、受信装置が受信した暗号化通信用データを自身が保持している複号用鍵データを用いて復号化することにより送信装置が予め記憶する通信用データを受信装置が共有し、この動作に引き続き共有した通信用データを用いて暗号通信を行なう暗号通信システムにおける機器認証方法であって、前記受信装置は第１アドレスデータと第２アドレスデータと復号用鍵データとからなるデータセットを１セット以上予め記憶しており、前記送信装置は第１アドレスデータから第２アドレスデータを特定できる第１アドレス付き第２アドレスデータと、第２アドレスデータから暗号化通信用データを特定できる第２アドレス付き暗号化通信用データとをそれぞれ複数予め記憶しており、前記受信装置から前記送信装置へ前記受信装置が予め記憶するデータセットの内の一のデータセットに属する第１アドレスデータを伝送する第１アドレスデータ伝送ステップと、前記送信装置において予め記憶している複数の第１アドレス付き第２アドレスデータから前記受信装置から前記第１アドレスデータ伝送ステップにより伝送された第１アドレスデータにより特定される第２アドレスデータを抽出する第２アドレスデータ抽出ステップと、前記受信装置における前記一のデータセットに属する第２アドレスデータと前記送信装置における前記第２アドレスデータ抽出ステップにより抽出された第２アドレスデータとが同じ値か否かを検証する検証ステップと、前記検証ステップにより同じ値であると検証された場合に前記送信装置において予め記憶している複数の第２アドレス付き暗号化通信用データから前記第２アドレスデータ抽出ステップにより抽出された第２アドレスデータにより特定される暗号化通信用データを抽出する暗号化通信用データ抽出ステップと、前記送信装置から前記受信装置へ前記暗号化通信用データ抽出ステップにより抽出された暗号化通信用データを伝送する暗号化通信用データ伝送ステップと、前記受信装置において前記暗号化通信用データ伝送ステップにより伝送された暗号化通信用データを前記一のデータセットに属する復号用鍵データを用いて復号化して通信用データを生成する復号化ステップとを有することを特徴とする。

【００４５】この方法によれば、受信装置（プレーヤ）が送信装置（鍵メディア）に送信する第１アドレスデータに対応する第２アドレスデータを保持している場合にのみ、送信装置（鍵メディア）が暗号化データを送信し受信装置（プレーヤ）が暗号化データを受信でき、この動作に引き続き暗号通信を行なうことができる。従って、受信装置（プレーヤ）は、正当な第１アドレスデータと第２アドレスデータとのセットとを保持していない限り暗号通信を行なえないので、適当な第１アドレスデータを送信装置（鍵メディア）に送信しても、正しい受信機になりすますことができなくなる。

【００４６】本発明に係る機器認証システムは、暗号通信の前に送信装置から受信装置へ通信用データが暗号化された暗号化通信用データを伝送して、受信装置が受信した暗号化通信用データを自身が保持している復号用鍵データを用いて復号化することにより送信装置が予め記憶する通信用データを受信装置が共有し、この動作に引き続き共有した通信用データを用いて暗号通信を行なう送信装置と受信装置とからなる機器認証システムであって、前記受信装置は、第１アドレスデータと第２アドレスデータと復号用鍵データとからなるデータセットを１セット以上予め記憶するデータセット記憶手段と、前記送信装置へ前記データセット記憶手段に記憶されたデータセットの内の一のデータセットに属する第１アドレスデータを送信する第１アドレスデータ送信手段と、前記一のデータセットに属する第２アドレスデータを元にして所定のデータ変換を施して、第１検証用データを生成する第１データ変換手段と、前記送信装置へ前記第１検証用データを送信する第１検証用データ送信手段と、前記送信装置から暗号化通信用データを受信する暗号化通信用データ受信手段と、前記暗号化通信用データ受信手段により受信された暗号化通信用データを前記一のデータセットに属する復号用鍵データを用いて復号化して通信用データを生成する復号化手段とを備え、前記送信装置は、第１アドレスデータから第２アドレスデータを特定できる第１アドレス付き第２アドレスデータと第２アドレスデータから暗号化通信用データを特定できる第２アドレス付き暗号化通信用データとをそれぞれ複数予め記憶する集合記憶手段と、前記受信装置から第１アドレスデータを受信する第１アドレスデータ受信手段と、前記集合記憶手段に記憶された複数の第１アドレス付き第２アドレスデータから前記受信装置から前記第１アドレスデータ受信手段により受信された第１アドレスデータにより特定される第２アドレスデータを抽出する第２アドレスデータ抽出手段と、前記受信装置から前記第１検証用データを受信する第１検証用データ受信手段と、前記第２アドレスデータ抽出手段により抽出された第２アドレスデータを元にして前記第１データ変換手段と同じデータ変換を施して第２検証用データを生成する第２データ変換手段と、前記第１検証用データ受信手段により受信された第１検証用データと前記第２データ変換手段により生成された第２検証用データとが同じ値か否かを検証する検証手段と、前記検証手段により同じ値であると検証された場合に予め記憶している複数の第２アドレス付き暗号化通信用データから前記第２アドレスデータ抽出手段により抽出された第２アドレスデータにより特定される暗号化通信用データを抽出する暗号化通信用データ抽出手段と、前記受信装置へ前記暗号化通信用デー

タ抽出手段により抽出された暗号化通信用データを送信する暗号化通信用データ送信手段とを備えることを特徴とする。

【００４７】この構成によれば、受信装置（プレーヤ）が送信装置（鍵メディア）に送信する第１アドレスデータに対応する第２アドレスデータを保持している場合にのみ、送信装置（鍵メディア）が暗号化データを送信し受信装置（プレーヤ）が暗号化データを受信でき、この動作に引き続き暗号通信を行なうことができる。従って、受信装置（プレーヤ）は、正当な第１アドレスデータと第２アドレスデータとのセットとを保持していない限り暗号通信を行なえないので、適当な第１アドレスデータを送信装置（鍵メディア）に送信しても、正しい受信機になりすますことができなくなる。

【００４８】本発明に係る受信装置は、暗号通信の前に送信装置から受信装置へ通信用データが暗号化された暗号化通信用データを伝送して、受信装置が受信した暗号化通信用データを自身が保持している復号用鍵データを用いて復号化することにより送信装置が予め記憶する通信用データを受信装置が共有し、この動作に引き続き共有した通信用データを用いて暗号通信を行なう機器認証システムにおける受信装置であって、第１アドレスデータと第２アドレスデータと復号用鍵データとからなるデータセットを１セット以上予め記憶するデータセット記憶手段と、前記送信装置へ前記データセット記憶手段に記憶されたデータセットの内の一のデータセットに属する第１アドレスデータを送信する第１アドレスデータ送信手段と、前記一のデータセットに属する第２アドレスデータを元にして所定のデータ変換を施して検証用データを生成するデータ変換手段と、前記送信装置へ前記検証用データを送信する検証用データ送信手段と、前記送信装置から暗号化通信用データを受信する暗号化通信用データ受信手段と、前記暗号化通信用データ受信手段により受信された暗号化通信用データを前記一のデータセットに属する復号用鍵データを用いて復号化して通信用データを生成する復号化手段とを備えることを特徴とする。

【００４９】この構成によれば、受信装置（プレーヤ）は送信装置（鍵メディア）に送信する第１アドレスデータに対応する第２アドレスデータを保持している場合にのみ、第２アドレスデータを元に検証用データを生成することができるので、正しい受信機になりすますことができなくなる。本発明に係る送信装置は、暗号通信の前に送信装置から受信装置へ通信用データが暗号化された暗号化通信用データを伝送して、受信装置が受信した暗号化通信用データを自身が保持している復号用鍵データを用いて復号化することにより送信装置が予め記憶する通信用データを受信装置が共有し、この動作に引き続き共有した通信用データを用いて暗号通信を行なう機器認証システムにおける送信装置であって、第１アドレスデータから第２アドレスデータを特定できる第１アドレス付き第２アドレスデータと、第２アドレスデータから暗号化通信用データを特定できる第２アドレス付き暗号化通信用データとをそれぞれ複数予め記憶する集合記憶手段と、前記受信装置から第１アドレスデータを受信する第１アドレスデータ受信手段と、前記集合記憶手段に記憶された複数の第１アドレス付き第２アドレスデータから前記受信装置から前記第１アドレスデータ受信手段により受信された第１アドレスデータにより特定される第２アドレスデータを抽出する第２アドレスデータ抽出手段と、前記受信装置から前記第１検証用データを受信する検証用データ受信手段と、前記第２アドレスデータ抽出手段により抽出された第２アドレスデータを元にして所定のデータ変換を施して第２検証用データを生成するデータ変換手段と、前記検証用データ受信手段により受信された第１検証用データと前記データ変換手段により生成された第２検証用データとが同じ値か否かを検証する検証手段と、前記検証手段により同じ値であると検証された場合に予め記憶している複数の第２アドレス付き暗号化通信用データから前記第２アドレスデータ抽出手段により抽出された第２アドレスデータにより特定される暗号化通信用データを抽出する暗号化通信用データ抽出手段と、前記受信装置へ前記暗号化通信用データ抽出手段により抽出された暗号化通信用データを送信する暗号化通信用データ送信手段とを備えることを特徴とする。

【００５０】この構成によれば、送信装置（鍵メディア）は、受信装置（プレーヤ）から正しい検証用データを受信した場合にのみ暗号化データを送信しこの動作に引き続き暗号通信を行なうことができるので、正しい検証用データを送信しない受信装置（プレーヤ）とは暗号通信を行なわないので安全である。本発明に係る受信装置側のプログラムを記録したコンピュータ読み取り可能な記録媒体は、暗号通信の前に送信装置から受信装置へ通信用データが暗号化された暗号化通信用データを伝送して、受信装置が受信した暗号化通信用データを自身が保持している復号用鍵データを用いて復号化することにより送信装置が予め記憶する通信用データを受信装置が共有し、この動作に引き続き共有した通信用データを用いて暗号通信を行なう機器認証システムにおける受信装置側のプログラムを記録したコンピュータ読み取り可能な記録媒体であって、前記受信装置は第１アドレスデータと第２アドレスデータと復号用鍵データとからなるデータセットを１セット以上予め記憶しており、コンピュータに、前記送信装置へ前記受信装置が予め記憶するデータセットの内の一のデータセットに属する第１アドレスデータを送信する第１アドレスデータ送信ステップと、前記一のデータセットに属する第２アドレスデータを元にして所定のデータ変換を施して検証用データを生成するデータ変換ステップと、前記送信装置へ前記検証

用データを送信する検証用データ送信ステップと、前記送信装置から暗号化通信用データを受信する暗号化通信用データ受信ステップと、前記暗号化通信用データ受信ステップにより受信された暗号化通信用データを前記一のデータセットに属する復号用鍵データを用いて復号化して通信用データを生成する復号化ステップとを実行させることを特徴とする。

【００５１】このプログラムによれば、受信装置（プレーヤ）は送信装置（鍵メディア）に送信する第１アドレスデータに対応する第２アドレスデータを保持している場合にのみ、第２アドレスデータを元に検証用データを生成することができるので、正しい受信機になりすますことができなくなる。本発明に係る送信装置側のプログラムを記録したコンピュータ読み取り可能な記録媒体は、暗号通信の前に送信装置から受信装置へ認証用データが暗号化された暗号化認証用データを伝送して、受信装置が受信した暗号化認証用データを自身が保持している復号用鍵データを用いて復号化することにより送信装置が予め記憶する認証用データを受信装置が共有し、この動作に引き続き共有した認証用データを用いて暗号通信を行なう機器認証システムにおける送信装置側のプログラムを記録したコンピュータ読み取り可能な記録媒体であって、前記送信装置は第１アドレスデータから第２アドレスデータを特定できる第１アドレス付き第２アドレスデータと第２アドレスデータから暗号化通信用データを特定できる第２アドレス付き暗号化通信用データとをそれぞれ複数予め記憶しており、コンピュータに、前記受信装置から第１アドレスデータを受信する第１アドレスデータ受信ステップと、前記受信装置が予め記憶している複数の第１アドレス付き第２アドレスデータから前記受信装置から前記第１アドレスデータ受信ステップにより受信された第１アドレスデータにより特定される第２アドレスデータを抽出する第２アドレスデータ抽出ステップと、前記受信装置から前記第１検証用データを受信する検証用データ受信ステップと、前記第２アドレスデータ抽出ステップにより抽出された第２アドレスデータを元にして所定のデータ変換を施し、第２検証用データを生成するデータ変換ステップと、前記検証用データ受信ステップにより受信された第１検証用データと前記データ変換ステップにより生成された第２検証用データとが同じ値か否かを検証する検証ステップと、前記検証ステップにより同じ値であると検証された場合に予め記憶している複数の第２アドレス付き暗号化通信用データから前記第２アドレスデータ抽出ステップにより抽出された第２アドレスデータにより特定される暗号化通信用データを抽出する暗号化通信用データ抽出ステップと、前記受信装置へ前記暗号化通信用データ抽出ステップにより抽出された暗号化通信用データを送信する暗号化通信用データ送信ステップと実行させることを特徴とする送信装置側のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【００５２】このプログラムによれば、送信装置（鍵メディア）は、受信装置（プレーヤ）から正しい検証用データを受信した場合にのみ暗号化データを送信しこの動作に引き続き暗号通信を行なうことができるので、正しい検証用データを送信しない受信装置（プレーヤ）とは暗号通信を行なわないので安全である。また、機器認証方法において、前記検証ステップは、前記受信装置内又は前記送信装置内で乱数データを発生させ発生させた乱数データを他方に伝送することにより同じ乱数データを共有する乱数データ共有サブステップと、前記受信装置において、前記一のデータセットに属する第２アドレスデータと前記共有した乱数データとに所定のデータ変換を施して第１検証用データを生成する第１データ変換サブステップと、前記受信装置から前記送信装置へ前記第１検証用データを伝送する第１検証用データ伝送サブステップと、前記送信装置において、前記第２アドレスデータ抽出ステップにより抽出された第２アドレスデータと前記共有した乱数データとに前記第１データ変換サブステップと同じデータ変換を施して第２検証用データを生成する第２データ変換サブステップと、前記送信装置において、前記第１検証用データと前記第２検証用データとが同じ値か否かを検証する検証サブステップとを有することを特徴とすることもできる。

【００５３】また、機器認証システムにおいて、前記受信装置が備える前記第１データ変換手段は、前記送信装置から乱数データを受信する乱数データ受信手段を含み、前記第１データ変換手段は、前記一のデータセットに属する第２アドレスデータと前記乱数データ受信手段により受信された乱数データとを元にして所定のデータ変換を施して第１検証用データを生成し、前記送信装置が備える前記第２データ変換手段は、乱数データを発生させ発生させた乱数データを前記受信装置に送信する乱数データ発生送信手段を含み、前記第２データ変換手段は、前記第２アドレスデータ抽出手段により抽出された第２アドレスデータと前記乱数データ発生送信手段により発生させた乱数データとを元にして所定のデータ変換を施して第２検証用データを生成することを特徴とすることもでき、また、前記受信装置が備える前記第１データ変換手段は、乱数データを発生させ発生させた乱数データを前記送信装置に送信する前記乱数データ発生送信手段を含み、前記第１データ変換手段は、前記一のデータセットに属する第２アドレスデータと前記乱数データ発生送信手段により発生させた乱数データとを元にして所定のデータ変換を施して第１検証用データを生成し、前記送信装置が備える前記第２データ変換手段は、前記受信装置から乱数データを受信する乱数データ受信手段を含み、前記第２データ変換手段は、前記第２アドレスデータ抽出手段により抽出された第２アドレスデータと前記乱数データ受信手段により受信された乱数データと

を元にして所定のデータ変換を施して第２検証用データを生成することを特徴とすることもできる。

【００５４】また、受信装置において、前記データ変換手段は、前記送信装置から乱数データを受信する乱数データ受信手段を含み、前記データ変換手段は、前記一のデータセットに属する第２アドレスデータと前記乱数データ受信手段により受信された乱数データとを元にして所定のデータ変換を施して検証用データを生成することを特徴とすることもでき、また、前記データ変換手段は、乱数データを発生させ発生させた乱数データを前記送信装置に送信する乱数データ発生送信手段を含み、前記データ変換手段は、前記一のデータセットに属する第２アドレスデータと前記乱数データ発生送信手段により発生させた乱数データとを元にして所定のデータ変換を施して検証用データを生成することを特徴とすることもできる。

【００５５】また、送信装置において、前記データ変換手段は、乱数データを発生させ発生させた乱数データを前記受信装置に送信する乱数データ発生送信手段を含み、前記データ変換手段は、前記第２アドレスデータ抽出手段により抽出された第２アドレスデータと前記乱数データ発生送信手段により発生させた乱数データとを元にして所定のデータ変換を施して第２検証用データを生成することを特徴とすることもでき、また、前記データ変換手段は、前記受信装置から乱数データを受信する乱数データ受信手段を含み、前記データ変換手段は、前記第２アドレスデータ抽出手段により抽出された第２アドレスデータと前記乱数データ受信手段により受信された乱数データとを元にして所定のデータ変換を施して第２検証用データを生成することを特徴とすることもできる。

【００５６】これによって、第２アドレスデータを乱数データを用いてデータ変換して伝送するので、通信路上のデータが第三者によって傍受されたとしても第２アドレスデータを知られることがなく安全である。

【図面の簡単な説明】

【図１】本実施の形態に係る暗号化通信システムの構成を示す図である。

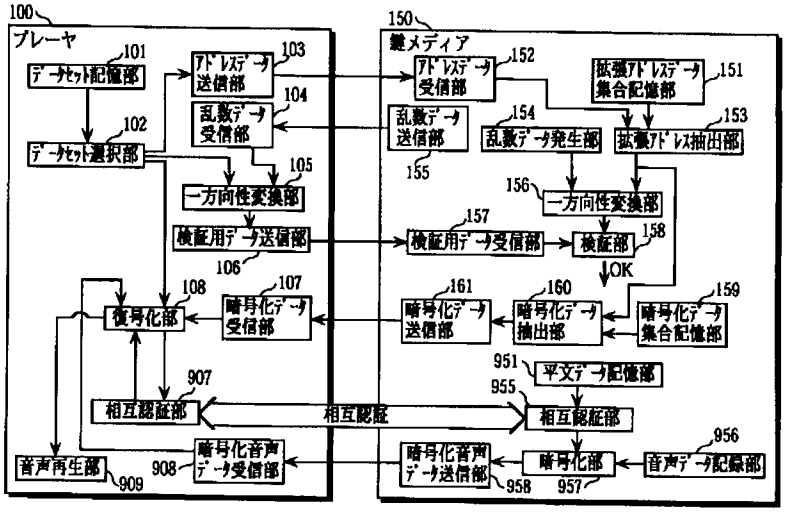
【図２】本実施の形態の暗号化通信システムの動作の一例を示す図である。

【図３】従来の暗号化通信における機器認証処理の概略を説明する為の暗号化通信システムを示す図である。

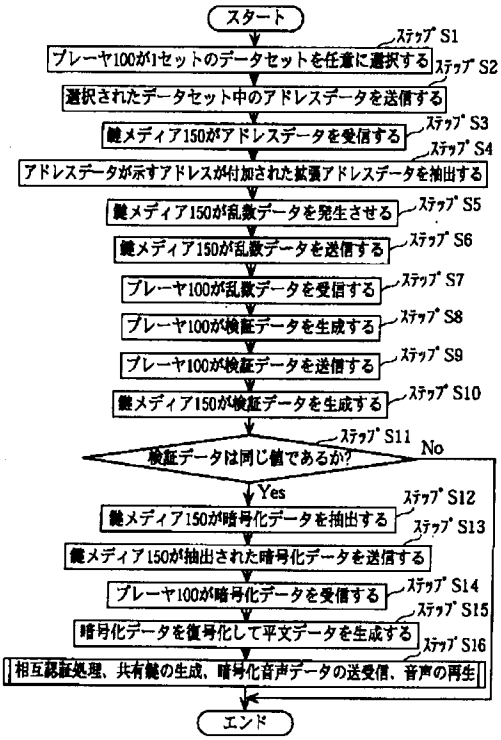
【符号の説明】

１００　プレーヤ
１０１　データセット記憶部
１０２　データセット選択部
１０３　アドレスデータ送信部
１０４　乱数データ受信部
１０５　一方向性変換部
１０６　検証用データ送信部
１０７　暗号化データ受信部
１０８　復号化部
９０７　相互認証部
９０８　暗号化音声データ受信部
９０９　音声再生部
１５０　鍵メディア
１５１　拡張アドレスデータ集合記憶部
１５２　アドレスデータ受信部
１５３　拡張アドレスデータ抽出部
１５４　乱数データ発生部
１５５　乱数データ送信部
１５６　一方向性変換部
１５７　検証用データ受信部
１５８　検証部
１５９　暗号化データ集合記憶部
１６０　暗号化データ抽出部
１６１　暗号化データ送信部
９５５　相互認証部
９５６　音声データ記録部
９５７　暗号化部
９５８　暗号化音声データ送信部

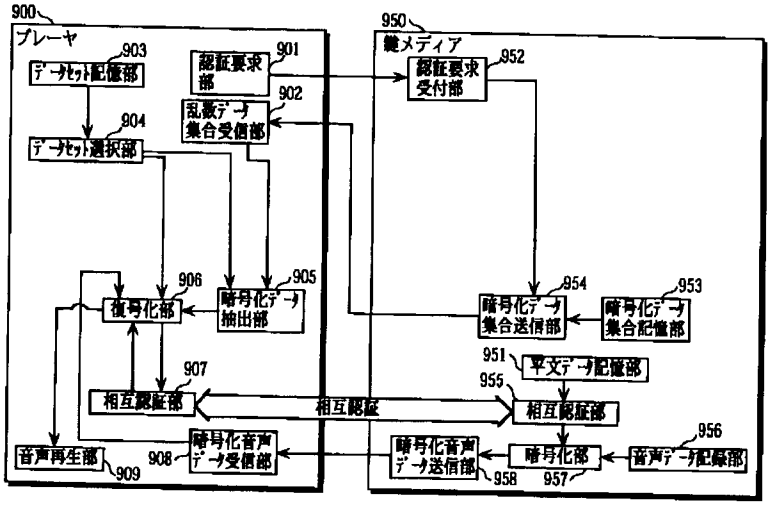
【図１】


100
プレーヤ
101
データセット記憶部
102
データセット選択部
103
アドレスデータ送信部
104
乱数データ受信部
105
一方向性変換部
106
検証用データ送信部
107
暗号化データ受信部
108
復号化部
907
相互認証部
暗号化音声データ受信部
908
音声再生部
909
150
鍵メディア
152
アドレスデータ受信部
151
拡張アドレスデータ集合記憶部
154
乱数データ発生部
153
拡張アドレス抽出部
155
乱数データ送信部
156
一方向性変換部
157
検証用データ受信部
158
検証部
OK
161
暗号化データ送信部
160
暗号化データ抽出部
159
暗号化データ集合記憶部
951
平文データ記憶部
955
相互認証部
相互認証
暗号化音声データ送信部
958
暗号化部
957
音声データ記録部
956

【図２】


スタート
ステップ S1
プレーヤ100が1セットのデータセットを任意に選択する
ステップ S2
選択されたデータセット中のアドレスデータを送信する
ステップ S3
鍵メディア150がアドレスデータを受信する
ステップ S4
アドレスデータが示すアドレスが付加された拡張アドレスデータを抽出する
ステップ S5
鍵メディア150が乱数データを発生させる
ステップ S6
鍵メディア150が乱数データを送信する
ステップ S7
プレーヤ100が乱数データを受信する
ステップ S8
プレーヤ100が検証データを生成する
ステップ S9
プレーヤ100が検証データを送信する
ステップ S10
鍵メディア150が検証データを生成する
ステップ S11
検証データは同じ値であるか?
No
Yes
ステップ S12
鍵メディア150が暗号化データを抽出する
ステップ S13
鍵メディア150が抽出された暗号化データを送信する
ステップ S14
プレーヤ100が暗号化データを受信する
ステップ S15
暗号化データを復号化して平文データを生成する
ステップ S16
相互認証処理、共有鍵の生成、暗号化音声データの送受信、音声の再生
エンド

【図３】



フロントページの続き

Ｆターム(参考)　5B017 AA03 BA07 BB09 CA16
5J104 AA07 AA13 AA16 EA04 EA24
KA02 KA03 KA06 KA10 NA02
NA27 PA14
9A001 BB03 BB04 EE02 EE03 GG22
JJ18 KK56 LL03